Operating Instructions
Security Guide

Read this manual carefully before you use this machine and keep it handy for future reference. For safe and correct use, be sure to read "Safety Information" before using the machine.

Introduction

This manual contains detailed instructions and notes on the operation and use of this machine. For your safety and benefit, read this manual carefully before using the machine. Keep this manual in a handy place for quick reference.

Do not copy or print any item for which reproduction is prohibited by law.

Copying or printing the following items is generally prohibited by local law:

bank notes, revenue stamps, bonds, stock certificates, bank drafts, checks, passports, driver's licenses.

The preceding list is meant as a guide only and is not inclusive. We assume no responsibility for its completeness or accuracy. If you have any questions concerning the legality of copying or printing certain items, consult with your legal advisor.

Important

Contents of this manual are subject to change without prior notice. In no event will the company be liable for direct, indirect, special, incidental, or consequential damages as a result of handling or operating the machine.

Trademarks

Microsoft®, Windows® and Windows NT® are registered trademarks of Microsoft Corporation in the United States and/or other countries.

AppleTalk, EtherTalk, are registered trademarks of Apple Computer, Inc.

Bonjour is a trademark of Apple Computer Inc.

PostScript® and Acrobat® are registered trademarks of Adobe Systems, Incorporated.

NetWare is a registered trademarks of Novell, Inc.

Bluetooth is a Trademark of the Bluetooth SIG, Inc. (Special Interest Group) and licensed to Ricoh Company Limited.

PictBridge is a trademark.

Other product names used herein are for identification purposes only and might be trademarks of their respective companies. We disclaim any and all rights to those marks.

The proper names of the Windows operating systems are as follows:

- The product name of Windows® 95 is Microsoft® Windows 95.
- The product name of Windows® 98 is Microsoft® Windows 98.
- The product name of Windows® Me is Microsoft® Windows Millennium Edition (Windows Me).
- The product names of Windows® 2000 are as follows:
  Microsoft® Windows® 2000 Advanced Server
  Microsoft® Windows® 2000 Server
  Microsoft® Windows® 2000 Professional
- The product names of Windows® XP are as follows:
  Microsoft® Windows® XP Professional
  Microsoft® Windows® XP Home Edition
- The product names of Windows Server® 2003 are as follows:
  Microsoft® Windows Server® 2003 Standard Edition
  Microsoft® Windows Server® 2003 Enterprise Edition
  Microsoft® Windows Server® 2003 Web Edition
- The product names of Windows NT® 4.0 are as follows:
  Microsoft® Windows NT® Server 4.0
  Microsoft® Windows NT® Workstation 4.0

Notes

Some illustrations in this manual might be slightly different from the machine.

Certain options might not be available in some countries. For details, please contact your local dealer.

Manuals for This Printer

For particular functions, see the relevant parts of the manual.

❖ **Safety Information**
Provides information on safe usage of this machine. To avoid injury and prevent damage to the machine, be sure to read this.

❖ **Quick Installation Guide**
Contains procedures for removing the printer from its box, connecting it to a computer, and installing its driver.

❖ **Hardware Guide**
Contains information about paper and procedures such as installing options, replacing consumables, responding to error messages, and resolving jams.

❖ **Software Guide**
Contain procedures for using this machine in a network environment, utilizing the software, and using security functions.

❖ **Security Guide (This manual)**
This manual is for administrators of the machine. It explains security functions that the administrators can use to protect data from being tampered, or prevent the machine from unauthorized use. Also refer to this manual for the procedures for registering administrators, as well as setting user and administrator authentication.

Note

❒ Manuals provided are specific to machine types.

❒ Adobe Acrobat Reader/Adobe Reader must be installed in order to view the manuals as PDF files.

Product name	General name
DeskTopBinder Lite and DeskTopBinder Professional *1	DeskTopBinder

*1 Optional

TABLE OF CONTENTS

1. Getting Started

2. Authentication and its Application

3. Preventing Information Leaks

4. Managing Access to the Printer

5. Enhanced Network Security

6. Specifying the Extended Security Functions

7. Troubleshooting

8. Appendix

How to Read This Manual

Symbols

This manual uses the following symbols:

⚠ WARNING:

Indicates important safety notes.

Ignoring these notes could result in serious injury or death. Be sure to read these notes. They can be found in the Safety Information.

⚠ CAUTION:

Indicates important safety notes.

Ignoring these notes could result in moderate or minor injury, or damage to the printer or to property. Be sure to read these notes. They can be found in the Safety Information.

Important

Indicates points to pay attention to when using the machine, and explanations of likely causes of paper misfeeds, damage to originals, or loss of data. Be sure to read these explanations.

Note

Indicates supplementary explanations of the printer's functions, and instructions on resolving user errors.

Reference

This symbol is located at the end of sections. It indicates where you can find further relevant information.

[ ]

Indicates the names of keys that appear on the printer's display panel.

【 】

Indicates the names of keys on the printer's control panel.

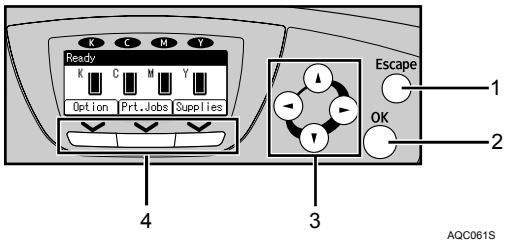
Display

The display panel shows printer status, error messages, and function menus.

Important

❒ A force or impact of more than 30 N (about 3 kgf) will damage the display.

Reading the Display and Using Panel Keys



1. 【Escape】 key

Press to cancel an operation or return to the previous display.

2. 【OK】 key

Press to set a selected item or entered numeric value.

3. Scroll keys

Press to move the cursor in each direction, step by step.

When the 【▲】, 【▼】, 【►】, or 【◄】 key appears in this manual, press the scroll key of the same direction.

4. Selection keys

Correspond to the function items at the bottom line on the display.

Example: In the initial screen, when the instruction "press **[Option]**" appears in this manual, press the left selection key.

Enhanced Security

This printer's security function can be enhanced through the management of the printer and its users using the improved authentication functions.

By specifying access limits on the printer's functions and the documents and data stored in the printer, you can prevent information leaks and unauthorized access.

Data encryption can prevent unauthorized data access and tampering via the network.

❖ **Authentication and Access Limits**

Using authentication, administrators manage the printer and its users. To enable authentication, information about both administrators and users must be registered in order to authenticate users via their login user names and passwords.

Four types of administrator manage specific areas of printer usage, such as settings and user registration.

Access limits for each user are specified by the administrator responsible for user access to printer functions and documents and data stored in the printer.

Reference

For details, see p.13 "Administrators".

❖ **Encryption Technology**

This printer can establish secure communication paths by encrypting transmitted data and passwords.

Glossary

❖ **Administrator**

There are four types of administrator according to the administered function: machine administrator, network administrator, file administrator, and user administrator. We recommend only one person take each administrator role. You can spread the workload and limit unauthorized operation by a single administrator.

Basically, administrators make printer settings and manage the printer; they cannot perform normal operations.

❖ **User**

A user performs normal operations on the printer.

❖ **File Creator (Owner)**

This is a user who has created and stored locked print and other files under the printer and who can view, edit, and delete those files.

❖ **Registered User**

This is a user whose personal information is registered in the address book. The registered user is the user who knows the login user name and password.

❖ **Administrator Authentication**

Administrators are authenticated by means of the login user name and login password supplied by the administrator when specifying the printer's settings or accessing the printer over the network.

❖ **User Authentication**

Users are authenticated by means of the login user name and login password supplied by the user when specifying the printer's settings or accessing the printer over the network.

The user's login user name and password are stored in the printer's address book. The personal information can be obtained from the Windows domain controller (windows authentication), LDAP Server (LDAP authentication), or Integration Server (Integration Server Authentication) connected to the printer via the network.

❖ **Login**

This action is required for administrator authentication and user authentication. Enter your login user name and login password on the printer's control panel.

A login user name and login password may also be supplied when accessing the printer over the network or using such utilities as Web Image Monitor and SmartDeviceMonitor for Admin.

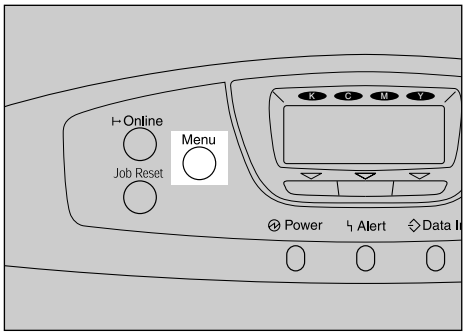
❖ **Logout**

This action is required with administrator and user authentication. This action is required when you have finished using the printer or changing the settings.

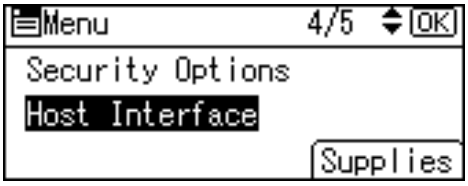
Setting Up the Printer

You can set the SSL. You can improve the security level by setting the SSL.
If you want higher security, make the following setting before using the printer:

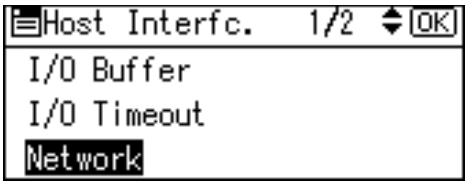
1 **Press the [Menu] key.**



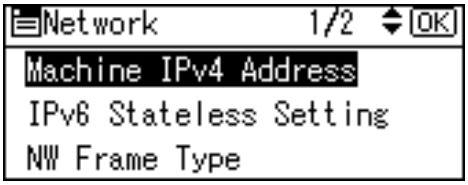
2 **Select [Host Interface] using the [▲] or [▼] key, and then press the [OK] key.**



3 **Select [Network] using the [▲] or [▼] key, and then press the [OK] key.**



4 **Select [Machine IPv4 Address] using the [▲] or [▼] key, and then press the [OK] key.**



5 Specify IP Address.

For details, see the Quick Installation Guide.

6 Connect the printer to the network.

7 Start the Web Image Monitor, and then log on to the printer as the administrator.

For details, see p.7 “Logging in Web Image Monitor”.

8 Install the server certificate.

For details, see Software Guide.

9 Enable secure sockets layer (SSL).

For details, see p.71 “Protection Using Encryption”.

10 Enter the administrator’s user name and password.

During steps 6 to 9, the administrator’s default account (user name: admin, password: blank) in unencrypted form will be vulnerable to network interception, and this account may be used for breaking into the printer over the network.

If you consider this risky, we recommend that you specify a temporary administrator password between steps 1 and 6.

Reference

p.21 “Registering the Administrator”

p.43 “Login (Using Web Image Monitor)”

p.71 “Protection Using Encryption”

Logging in Web Image Monitor

Specify the authentications using Web Image Monitor.

❖ Recommended Web browser

- Windows:
  Internet Explorer 5.5 SP2 or higher
  Firefox 1.0 or higher
- Mac OS:
  Firefox 1.0 or higher
  Safari 1.0, 1.2, 2.0 (412.2) or higher

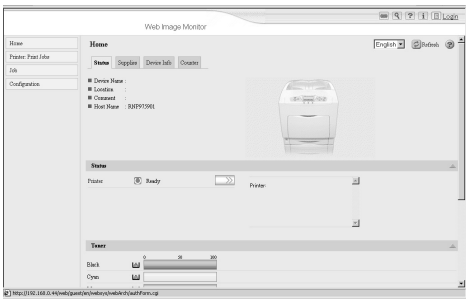
Note

❒ Safari cannot be used on Mac OS X 10.4.1.
❒ If the previous versions of the Web browser above are used or JavaScript and cookies are not enabled with the Web browser used, display and operation problems may occur.
❒ The previous page may not appear even after the back button of a Web browser is clicked. If this happens, click the refresh button of a Web browser.
❒ Updating the printer information is not automatically performed. Click **[Refresh]** in the display area to update the printer information.
❒ We recommend using Web Image Monitor in the same network.
❒ You cannot access to the printer from outside the firewall.
❒ When using the printer under DHCP, the IPv4 address may be automatically changed by the DHCP server settings. Enable DDNS setting on the printer, and then connect using the printer's host name. Alternatively, set a static IPv4 address to the DHCP server.
❒ If the HTTP port is disabled, connection to the printer using the printer's URL cannot be established. SSL setting must be enabled on this printer. For details, consult your network administrator.
❒ When using the SSL encryption protocol, enter "https://(printer's address)/". Internet Explorer must be installed on your computer. Use the most recent available version. We recommend Internet Explorer 6.0 or later.

Displaying Top Page

1 Start your Web browser.

2 Enter "http://(printer's address)/" in the address bar of a Web browser.

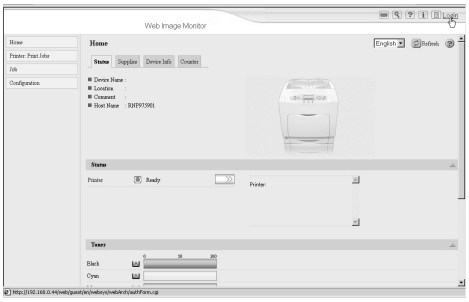


Top Page of Web Image Monitor appears.
If the printer's host name has been registered on the DNS or WINS server, you can enter it.
When setting SSL, a protocol for encrypted communication, under environment which server authentification is issued , enter "https://(printer's address)/".

Logging in (Administrator mode)

1 **Click [Login].**

The window for entering the login user name and password for the Web Image Monitor administrator appears.



2 **Enter a login user name and pass word, and then click [Login].**

To use the default account, enter "admin" as user name, and leave the password blank.

Note

❒ The procedure may differ depending on the Web browser used.

Logging off (Administrator mode)

1 **Click [Logout] to log off.**

Note

❒ When you log on and made the setting, always click **[Logout]**.

Security Measures Provided by this Printer

Using Authentication and Managing Users

❖ **Enabling Authentication**

To control administrators' and users' access to the printer, perform administrator authentication and user authentication using login user names and login passwords. To perform authentication, the authentication function must be enabled.

Reference

For details, see p.18 "Enabling Authentication".

❖ **Specifying Which Functions are Available**

This can be specified by the user administrator. Specify the functions available to registered users. By making this setting, you can limit the functions available to users.

Reference

For details, see p.59 "Specifying Which Functions are Available".

Preventing Information Leaks

❖ **Guarding Against Unauthorized Copying (Unauthorized Copy Prevention)**
Using the printer driver, you can embed mask and pattern in the printed document.

Reference
For details, see p.45 “Guarding Against Unauthorized Copying”.

❖ **Guarding Against Unauthorized Copying (Data Security for Copying)**
Using the printer driver to enable data security for the copying function, you can print a document with an embedded pattern of hidden text.
To gray out the copy or stored file of a copy-guarded document when the document is copied or stored , the optional security module is required.

Reference
For details, see p.45 “Guarding Against Unauthorized Copying”.

❖ **Printing confidential files**
Using the printer’s Locked Print, you can store files in the printer as confidential files and then print them. You can print a file using the printer’s control panel and collect it on the spot to prevent others from seeing it.

Reference
For details, see p.50 “Printing a Confidential Document”.

❖ **Protecting Registered Information in the Address Book**
You can specify who is allowed to access the data in the address book. You can prevent the data in the address book being used by unregistered users.
To protect the data from unauthorized reading, you can also encrypt the data in the address book.

Reference
For details, see p.55 “Protecting the Address Book”.

❖ **Managing Log Files**
You can improve data security by deleting log files stored in the printer. By transferring the log files, you can check the history data and identify unauthorized access.
To transfer the log data, the log collection server is required.

Reference
For details, see p.60 “Managing Log Files”.

Limiting and Controlling Access

❖ **Preventing Modification or Deletion of Stored Data**
To prevent modification of stored data, you can set password to them.

❖ **Preventing Modification of Printer Settings**
The printer settings that can be modified depend on the type of administrator account.
Register the administrators so that users cannot change the administrator settings.

Reference
For details, see p.57 “Preventing Modification of printer Settings”.

❖ **Limiting Available Functions**
To prevent unauthorized operation, you can specify who is allowed to access each of the printer's functions.

Reference
For details, see p.59 “Limiting Available Functions”.

Enhanced Network Security

❖ **Preventing Unauthorized Access**
You can limit IP addresses or disable ports to prevent unauthorized access over the network and protect the address book, stored files, and default settings.

Reference
For details, see p.63 “Preventing Unauthorized Access”.

❖ **Encrypting Transmitted Passwords**
Prevent login passwords, group passwords for PDF files, and IPP authentication passwords being revealed by encrypting them for transmission.
Also, encrypt the login password for administrator authentication and user authentication.

Reference
For details, see p.67 “Encrypting Transmitted Passwords”.

❖ **Safer Communication Using SSL**
When you access the printer using a Web Image Monitor or IPP, you can establish encrypted communication using SSL. When you access the printer using an application such as SmartDeviceMonitor for Admin, you can establish encrypted communication using SNMPv3 or SSL.
To protect data from interception, analysis, and tampering, you can install a server certificate in the printer, negotiate a secure connection, and encrypt transmitted data.

Reference
For details, see p.71 “Protection Using Encryption”.

2. Authentication and its Application

Administrators and Users

When controlling access using the authentication specified by an administrator, select the printer's administrator, enable the authentication function, and then use the printer.

The administrators manage access to the allocated functions, and users can use only the functions they are permitted to access. To enable the authentication function, the login user name and login password are required in order to use the printer.

Specify administrator authentication, and then specify user authentication.

Important

❒ If user authentication is not possible because of a problem with the optional hard disk or network, you can use the printer by accessing it using administrator authentication and disabling user authentication. Do this if, for instance, you need to use the printer urgently.

Reference

For details, see p.28 "Specifying Login User Name and Login Password".

Administrators

There are four types of administrator according to the administered function: machine administrator, network administrator, file administrator, and user administrator.

By sharing the administrative work among different administrators, you can spread the workload and limit unauthorized operation by a single administrator. You can also specify a supervisor who can change each administrator's password. Administrators are limited to managing the printer's settings and controlling user access. So they cannot use functions such as printing. To use such functions, you need to register a user in the address book and then be authenticated as the user.

Reference

For details, see p.21 "Registering the Administrator".

For details, See p.89 "Operations by the Supervisor".

❖ **User Administrator**

This is the administrator who manages personal information in the address book.

A user administrator can register/delete users in the address book or change users' personal information.

Users registered in the address book can also change and delete their own information. If any of the users forget their password, the user administrator can delete it and create a new one, allowing the user to access the printer again.

❖ **Machine Administrator**

This is the administrator who mainly manages the printer's default settings. You can set the printer so that the default for each function can only be specified by the machine administrator. By making this setting, you can prevent unauthorized people from changing the settings and allow the printer to be used securely by its many users.

❖ **Network Administrator**

This is the administrator who manages the network settings. You can set the printer so that network settings such as the IP address and settings for sending and receiving e-mail can only be specified by the network administrator. By making this setting, you can prevent unauthorized users from changing the settings and disabling the printer, and thus ensure correct network operation.

❖ **File Administrator**

This administrator manages stored files and can specify and delete passwords for locked print files and other files.

❖ **Supervisor**

The supervisor can delete an administrator's password and specify a new one. The supervisor cannot specify defaults or use normal functions. However, if any of the administrators forget their password and cannot access the printer, the supervisor can provide support.

Note

❒ All administrators are set as Administrator1 by default. Divide the administrator between 1 - 4 as need arise.

User

Users are managed using the personal information managed in the printer's address book.

By enabling user authentication, you can allow only people registered in the address book to use the printer. Users can be managed in the address book by the user administrator.

Reference

For details about registering users in the address book, see the SmartDeviceMonitor for Admin Help, or the Web Image Monitor Help.

The Management Function

The printer has an authentication function requiring a login user name and login password. By using the authentication function, you can specify access limits for individual users and groups of users. Using access limits, you can not only limit the printer's available functions but also protect the printer settings, files, and data stored in the printer.

Important

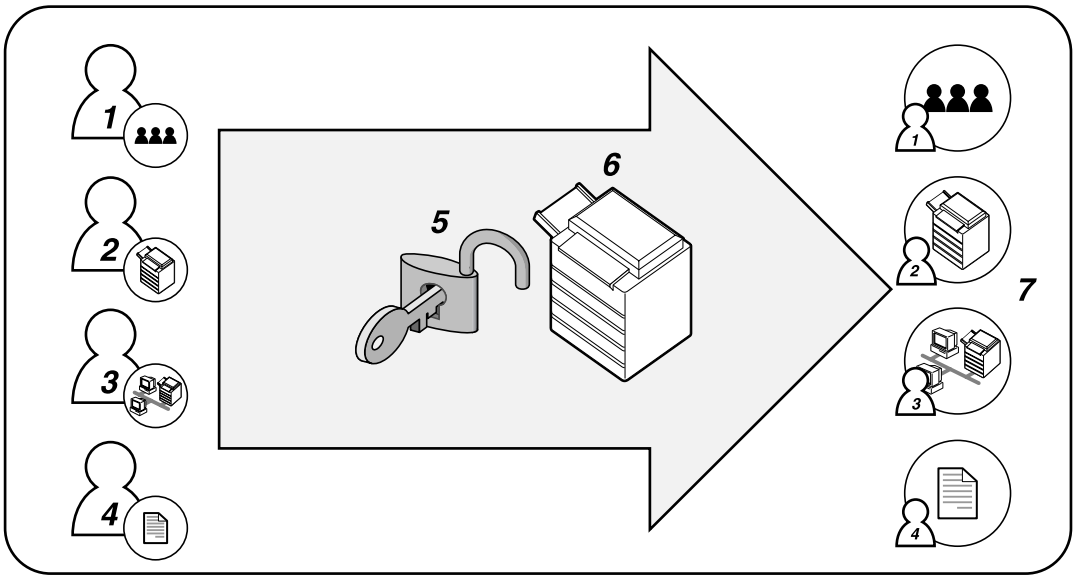
- ❒ If you have enabled **[Administrator Authentication Management]**, make sure not to forget the administrator login user name and login password. If an administrator login user name or login password is forgotten, a new password must be specified using the supervisor's authority.
- ❒ Be sure not to forget the supervisor login user name and login password. If you do forget them, a service representative will to have to return the printer to its default state. This will result in all data in the printer being lost and the service call may not be free of charge.

Reference

For details, see p.89 "Operations by the Supervisor".

About Administrator Authentication

There are four types of administrator according to the administered function: user administrator, machine administrator, network administrator, and file administrator.



AYJ002S

1. User Administrator

This administrator manages personal information in the address book. You can register/delete users in the address book or change users' personal information.

2. Machine Administrator

This administrator manages the printer'so default settings. You can set the printer so that the default such as data security for copying function and delete all logs can only be specified by the machine administrator.

3. Network Administrator

This administrator manages the network settings. You can set the printer so that network settings such as the IP address and settings for sending and receiving e-mail can only be specified by the network administrator only.

4. File Administrator

This administrator manages stored files and can specify and delete passwords for locked print files and other files.

5. Authentication

Administrators must enter their login user name and password to be authenticated.

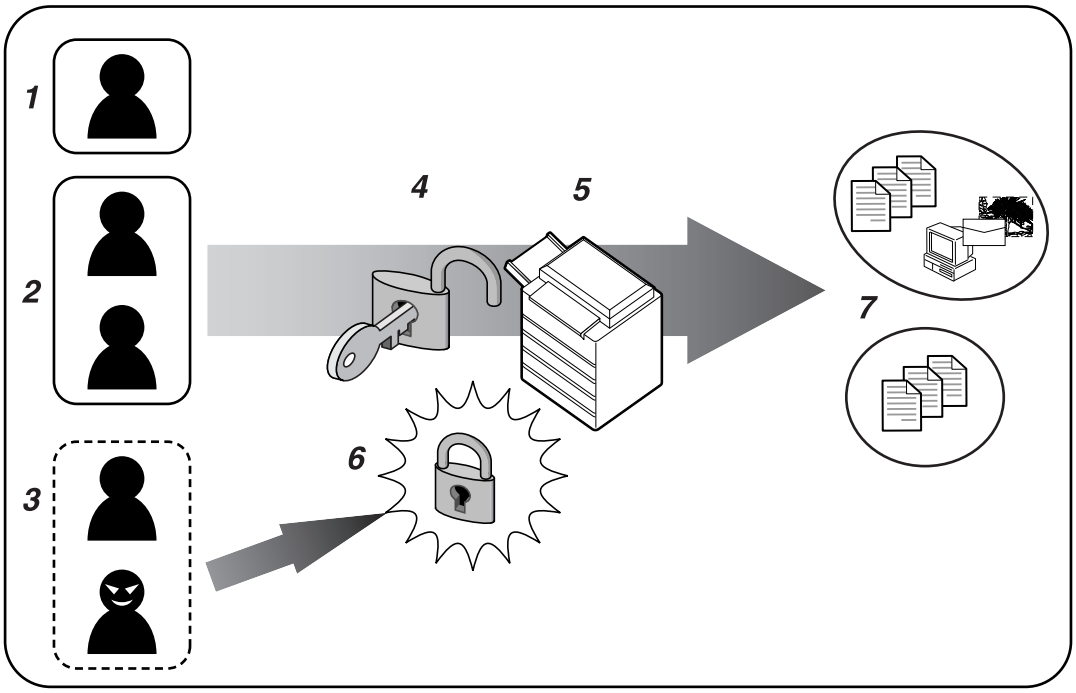
6. This printer

7. Administrators manage the printer'so settings and access limits. For details about each administrator, see p.13 "Administrators".

About User Authentication

This printer has an authentication function to prevent unauthorized access.

By using login user name and login password, you can specify access limits for individual users and groups of users.



1. User

A user performs normal operations on the printer, such as copying and printing.

2. Group

A group performs normal operations on the printer.

3. Unauthorized User

4. Authentication

Using a login user name and password, user authentication is performed.

5. This Printer

6. Access Limit

Using authentication, unauthorized users are prevented from accessing the printer.

7. Authorized users and groups can use only those functions permitted by the administrator.

Enabling Authentication

To control administrators' and users' access to the printer, perform administrator or user authentication using login user names and passwords. To perform authentication, the authentication function must be enabled. To specify authentication, you need to register administrators.

Reference

For details, see p.21 "Registering the Administrator".

Authentication Setting Procedure

Specify administrator authentication and user authentication according to the following chart:

Note

- ❒ To specify Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication, you must first specify administrator authentication.
- ❒ You can specify User Code Authentication without specifying administrator authentication.
- ❒ User Code Authentication is not the User Authentication at Administrator Authentication , so it can be used when there is no Administrator Authentication.

Administrator Authentication See p.19 "Specifying Administrator Privileges".	Specifying Administrator Privileges See p.19 "Specifying Administrator Privileges". Registering the Administrator See p.21 "Registering the Administrator".
User Authentication See p.18 "Enabling Authentication".	Specifying User Authentication ① Authentication that requires only the printer: • User Code Authentication See p.24 "User Code Authentication". • Basic Authentication See p.26 "Basic Authentication". ② Authentication that requires external devices: • Windows Authentication See p.29 "Windows Authentication". • LDAP Authentication See p.34 "LDAP Authentication". • Integration Server Authenticarion See p.37 "Integration Server Authentication".

Administrator Authentication

Administrators are handled differently from the users registered in the address book. When registering an administrator, you cannot use a login user name already registered in the address book. Windows Authentication, LDAP Authentication and Integration Server Authentication are not required for an administrator, so an administrator can log on even if the server is unreachable due to network problem.

Each administrator is identified by a login user name. One person can act as more than one type of administrator if multiple administrator authority is granted to a single login user name.

You can specify the login user name, login password, and encryption password for each administrator.

The encryption password is a password for performing encryption when specifying settings using Web Image Monitor or SmartDeviceMonitor for Admin.

The password registered in the printer must be entered when using applications such as SmartDeviceMonitor for Admin.

Administrators are limited to managing the printer'so settings and controlling user access. So they cannot use functions such as printing. To use such functions, you need to register a user in the address book and then be authenticated as the user.

Specify the administrator authentication using Web Image Monitor

Specifying Administrator Privileges

To specify administrator authentication, set Administrator Authentication Management to **[On]**.

To log on as an administrator, use the default login user name and login password.

The defaults are "admin" for the login name and blank for the password.

Important

❒ If you have enabled **[Administrator Authentication Management]**, make sure not to forget the administrator login user name and login password. If an administrator login user name or login password is forgotten, a new password must be specified using the supervisor'so authority.

Reference

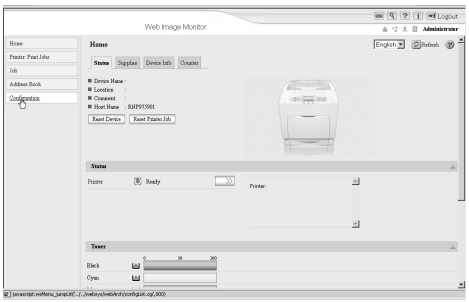
For details, see p.89 "Operations by the Supervisor".

Note

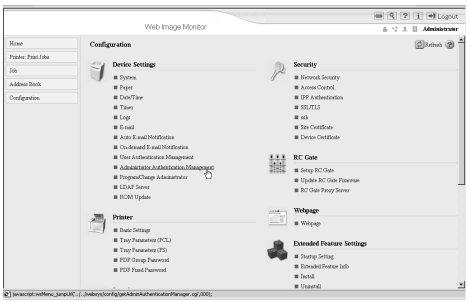
❒ For details about logging on and logging off with administrator authentication, see p.22 "Logging on Using Administrator Authentication", p.23 "Logging off Using Administrator Authentication".

1. Log on to Web Image Monitor in the administrator mode.

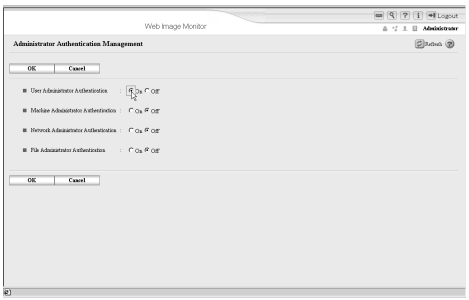
2. Click [Configuration].



3. Click [Administrator Authentication Management] in the "Device Settings" area.



4. Select [User Administrator Authentication], [Machine Administrator Authentication], [Network Administrator Authentication], or [File Administrator Authentication], and then press [OK].



5. Quit Web Image Monitor.

Registering the Administrator

If administrator authentication has been specified, it is recommended to assign each administrator role to a different person.

By sharing the administrative work among different administrators, you can spread the workload and limit unauthorized operation by a single administrator. You can register up to four login user names (Administrators 1 to 4) to which you can grant administrator privileges.

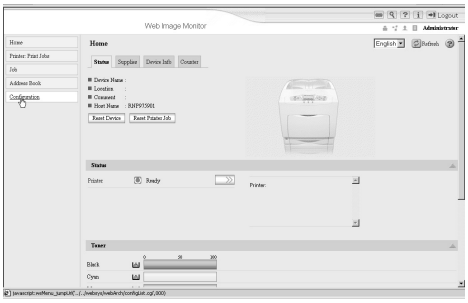
Administrator authentication is specified via Web Image Monitor.

Note

- ❒ You can use up to 32 alphanumeric characters and symbols when registering login user names and login passwords. Keep in mind that passwords are case-sensitive.
- ❒ You cannot include spaces, semicolons (;), or quotes (") in the user name, nor can you leave the user name blank.
- ❒ Do not use Japanese, Traditional Chinese, Simplified Chinese, or Hangul double-byte characters when entering the login user name or password. If you use multi-byte characters when entering the login user name or password, you cannot authenticate using Web Image Monitor.

1 **Log on to Web Image Monitor in the administrator mode.**

2 **Click [Configuration].**



3 **Click [Program/Change Administrator] in the "Device Settings" area.**

4 **Select the administrator type and administrator number.**

5 **Enter the [Login User Name] of the selected administrator number.**

6. **Click [Change] in the "Login Password" area.**
   The window for entering the password appears.
7. **Enter the password.**
8. **Re-enter the same password, and then click [OK].**
9. **Click [Change] in the "Encryption Password" area.**
   The window for entering the password appears.
10. **Enter the password.**
11. **Re-enter the same password, and then click [OK].**
12. **Click [OK].**
13. **Quit Web Image Monitor.**

Logging on Using Administrator Authentication

If administrator authentication has been specified, log on using an administrator's user name and password. This section describes how to log on.

Note

- To log on as an administrator, enter the administrator's login user name and login password.
- If you try to log on from an operating screen, "`Selected function cannot be used.`" appears. Press the **【Menu】** key to change the default.

1. **Press the【Menu】key.**
2. **Press【Login】.**
3. **Press【Text】.**
   The window for entering the login user name appears.
4. **Enter the login user name using the【▲】,【▼】,【◄】or【►】key, and then press [Exit].**
   When you log on to the printer for the first time as the administrator, enter "admin".
   A message window appears.
5. **Press [Text].**
   The window for entering the login password appears.
6. **Enter the password using the【▲】,【▼】,【◄】or【►】key, and then press [Exit].**
   If assigning the administrator for the first time, press **[OK]** without entering login password.
   "`Authenticating... Please wait.`" appears, followed by the screen for specifying the default.

Logging off Using Administrator Authentication

If administrator authentication has been specified, be sure to log off after completing settings. This section explains how to log off after completing settings.

1. **Press [Logout].**
2. **Press [Yes].**

Changing the Administrator

Change the administrator's login user name and login password. You can also assign each administrator's authority to the login user names "Administrator " to "Administrator 4" To combine the authorities of multiple administrators, assign multiple administrators to a single administrator.

For example, to allocate the machine administrator and user administrator access privileges to "Administrator 1", set machine administrator and user administrator to "Administrator 1" in "Permissions".

Specify using the Web Image Monitor.

1. **Log on to Web Image Monitor in the administrator mode.**
2. **Click [Configuration].**
3. **Click [Program/Change Administrator] in the "Device Settings" area.**
4. **Select [Administrator 1], [Administrator 2], [Administrator 3], or [Administrator 4], and then press [OK].**
5. **Quit Web Image Monitor.**

User Authentication

There are five types of user authentication method: user code authentication, basic authentication, Windows authentication, Integration Server Authentication, and LDAP authentication. To use user authentication, select an authentication method in Web Image Monitor, and then make the required settings for the authentication. The settings depend on the authentication method. To specify a user authentication setting other than User Code Authentication, the optional hard disk must be installed.

Note

❒ Under user code authentication, authentication is based on the user code. In contrast, under basic authentication, Windows authentication, and LDAP authentication, authentication is carried out for individual users.

User Code Authentication

This is an authentication method for limiting access to functions according to the user code. The same user code can be used by more than one user. For details about specifying user codes, see Web Image Monitor Help.

Limitation

❒ To control the use of DeskTopBinder for the delivery of files stored in the printer, select Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication.

Reference

For details about specifying the user code for the printer driver, see Software Guide or the printer driver Help.

Specifying User Code Authentication

This can be specified by the machine administrator.

1. **Log on to Web Image Monitor in the administrator mode.**
2. **Click [Configuration].**
3. **Click [Administrator Authentication Management] in the "Device Settings" area.**
4. **Click [On] in the "User Administrator Authentication" area, and then click [OK].**
5. **Click [User Authentication Management] in the "Device Settings" area.**
6. **Select [User Code] in the "User Authentication Management" list.**

   If you do not want to use user authentication management, select **[Off]**.
7. **Select the "Printer Job Authentication" level.**

Note

❒ If you select **[Entire]**, you cannot print using a printer driver or a device that does not support authentication. To print under an environment that does not support authentication, select **[Simple (All)]**.

❒ If you select **[Simple (Limitation)]**, you can specify clients for which printer job authentication is not required. Specify **[Parallel Interface (Simple)]**, **[USB (Simple)]** and the clients' IPv4 or IPv6 address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.

❒ If you select **[Simple (All)]** or **[Simple (Limitation)]**, you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the printer or if you do not require authentication for printing. However, note that, because the printer does not require authentication in this case, it may be used by unauthorized users.

If you select **[Entire]**, proceed to step ⓭.

If you select **[Simple (All)]** or **[Simple (Limitation)]**, proceed to step ❽.

Reference

For details, see p.39 "Printer Job Authentication Levels and Printer Job Types".

❽ **Select [Simple (Limitation)], and enter "Limitation Range".**

Specify the range in which **[Simple (Limitation)]** is applied to Printer Job Authentication.

If you specify IPv4 or IPv6 address range, proceed to step ❾.

If you specify **[USB (Simple)]**, proceed to step ⓫.

If you specify **[Parallel Interface (Simple)]**, proceed to step ⓾.

❾ **Select [IPv4 Address 1], [IPv4 Address 2], [IPv4 Address 3], or [IPv4 Address 4], and then enter the IPv4 address on the "Limitation Range (IPv4)" area.**

Be sure the number you enter for End IPv4 Address is larger than that for Start IPv4 Address.

If you want to use IPv6, specify the IPv6 address in the "Limitation Range (IPv6)" area.

❿ **Click [Apply] in the "Parallel Interface (Simple)" area.**

⓫ **Click [Apply] in the "USB (Simple)" area.**

⓬ **Select "Available Function".**

Select **[Black&White]**, **[Color]**, or **[PC Control]** when enabling color or black-and-white printing.

⓭ **Click [OK].**

The "Updating..." message appears.

⓮ **Click [OK] key.**

Configuration page appears.

⓯ **Quit Web Image Monitor.**

Note

❒ You can specify User Code Authentication without specifying administrator authentication.

❒ This can also be set using telnet.

Basic Authentication

Specify this authentication when using the printer's address book to authenticate for each user. Using basic authentication, you can not only manage the printer's available functions but also limit access to stored files and to the personal data in the address book. Under basic authentication, the administrator must specify the functions available to each user registered in the address book.

To perform Basic Authentication, the optional hard disk must be installed.

Specify the basic authentication using Web Image Monitor.

Specifying Basic Authentication

This can be specified by the machine administrator.

1. **Log on to Web Image Monitor in the administrator mode.**
2. **Click [Configuration].**
3. **Click [Administrator Authentication Management] in the "Device Settings" area.**
4. **Click [On] in the "User Administrator Authentication" area, and then click [OK].**
5. **Click [User Authentication Management], and then select "Basic Authentication" in the "User Authentication Management" list.**

   If you do not want to use user authentication management, select **[Off]**.

6. **Select the "Printer Job Authentication" level.**

Note

- If you select **[Entire]**, you cannot print using a printer driver or a device that does not support authentication. To print under an environment that does not support authentication, select **[Simple (All)]**.
- If you select **[Simple (Limitation)]**, you can specify clients for which printer job authentication is not required. Specify **[Parallel Interface (Simple)]**, **[USB (Simple)]** and the clients' IPv4 or IPv6 address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.
- If you select **[Simple (All)]** or **[Simple (Limitation)]**, you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the printer or if you do not require authentication for printing. However, note that, because the printer does not require authentication in this case, it may be used by unauthorized users.

If you select **[Entire]**, proceed to step 12.

If you select **[Simple (All)]** or **[Simple (Limitation)]**, proceed to step 7.

Reference

For details, see p.39 "Printer Job Authentication Levels and Printer Job Types".

7 **Select [Simple (Limitation)], and enter [Limitation Range].**

Specify the range in which **[Simple (Limitation)]** is applied to Printer Job Authentication.

If you specify IPv4 or IPv6 address range, proceed to step **8**.

If you specify "USB (Simple)", proceed to step **11**.

If you specify "Parallel Interface (Simple)", proceed to step **9**.

8 **Select [IPv4 Address 1], [IPv4 Address 2], [IPv4 Address 3], or [IPv4 Address 4], and then enter the IPv4 address on the "Limitation Range (IPv4)" area.**

Be sure the number you enter for End IPv4 Address is larger than that for Start IPv4 Address.

If you want to use IPv6, specify the IPv6 address in the "Limitation Range (IPv6)" area.

9 **Click [Apply] in the "Parallel Interface (Simple)" area.**

10 **Click [Apply] in the "USB (Simple)" area.**

11 **Select "Available Function".**

Clear the **[Black&White]** or **[Color]** check box when you want to limit the color or black-and-white printing.

The initially set value becomes default.

12 **Click [OK].**

"Updating..." message appears.

13 **Click [OK].**

Configuration page appears.

14 **Quit Web Image Monitor.**

Note

❒ This can also be set using Telnet.

Authentication Information Stored in the Address Book

This can be specified by the user administrator.

If you have specified User Authentication, you can specify access limits for individual users and groups of users. Specify the setting in the address book for each user.

Preparation

For details about logging on and logging off with administrator authentication, see p.22 "Logging on Using Administrator Authentication", p.23 "Logging off Using Administrator Authentication".

You need to register a user in the address book. For details about address book registration, see Web Image Monitor Help.

See p.59 "Limiting Available Functions".

Specifying Login User Name and Login Password

In **[User Authentication Management]**, specify the login user name and password.

1. **Log on to Web Image Monitor in the administrator mode.**
2. **Click [Address Book].**
   Address List screen appears.
3. **Select the user you want to specify, and then click [Change].**
   You can search using Name, Registration No., or User Code.
4. **Enter the "Login User Name" in the "Authentication Info at Login" area in the "Authentication Information" area.**
5. **Click [Change] in the "Login Password" area.**
6. **Enter the login password, and then click [OK].**
7. **Specify "Available Function".**
   The initial value is set at Basic Authentication. If the value is reset, the previous value will be overwritten.
8. **Click [Change] in "Access Privileges" in the "Protect Destination" area in the "Protection" area.**
9. **Select the usable level on both "Public" and "User/Group", and then click [OK].**
   When adding a changed user to the group, click **[Change]** in the "Add to Group" area, and then click **[OK]**.
10. **Click [Back].**
    Home page appears.

Windows Authentication

Specify this authentication when using the Windows domain controller to authenticate users who have their accounts on the directory server. Users cannot be authenticated if they do not have their accounts in the directory server. Under Windows authentication, you can specify the access limit for each group registered in the directory server. The address book stored in the directory server can be registered to the printer, enabling user authentication without first using the printer to register individual settings in the address book.

Important

❒ During Windows Authentication, data registered in the directory server is automatically registered in the printer. If user information on the server is changed, information registered in the printer may be overwritten when authentication is performed.

❖ Operational Requirements for Windows Authentication

- To specify Windows authentication, the following requirements are recommended:
  - The optional hard disk unit must be installed.
  - A domain controller has been set up in a designated domain.
  - This function is supported by the operating systems listed below. NTLM authentication is used for Windows authentication. To obtain user information when running Active Directory, use LDAP. If SSL is being used, this requires a version of Windows that supports TLS v1, SSL v2, or SSL v3.
    - Windows NT 4.0 Server
    - Windows 2000 Server
    - Windows Server 2003

Limitation

❒ If you have created a new user in the domain controller and selected **[User must change password at next logon]**, log on to the printer from the computer to change the password before logging on from the printer's control panel.

Note

❒ The first time you access the printer, you can use the functions available to your group. If you are not registered in a group, you can use the functions available under **[*Default Group]**. To limit which functions are available to which users, first make settings in advance in the address book.
❒ When accessing the printer subsequently, you can use all the functions available to your group and to you as an individual user.
❒ Enter the login password correctly, keeping in mind that it is case-sensitive.
❒ Users who are registered in multiple groups can use all the functions available to those groups.
❒ If you specify in the address book which functions are available to global group members, those settings have priority.
❒ A user registered in two or more global groups can use all the functions available to members of those groups.
❒ If the "Guest" account on the Windows server is enabled, even users not registered in the domain controller can be authenticated. When this account is enabled, users are registered in the address book and can use the functions available under **[*Default Group]**.

Specifying Windows Authentication

This can be specified by the machine administrator.

Specify the windows authentication using Web Image Monitor.

Note

❒ Under Windows Authentication, you can select whether or not to use secure sockets layer (SSL) authentication.

1 Log on to Web Image Monitor in the administrator mode.

2 Click [Configuration].

3 Click [Administrator Authentication Management] in the "Device Settings" area.

4 Click [On] in the "User Administrator Authentication" area, and then click [OK].

Configuration page appears.

5 Click [User Authentication Management] in the "Device Settings" area.

6 Select "Windows Authentication" in the "User Authentication Management" list.

If you do not want to use user authentication management, select **[Off]**.

7 Select the "Printer Job Authentication" level.

Note

❒ If you select **[Entire]**, you cannot print using a printer driver or a device that does not support authentication. To print under an environment that does not support authentication, select **[Simple (All)]**.

❒ If you select **[Simple (Limitation)]**, you can specify clients for which printer job authentication is not required. Specify **[Parallel Interface (Simple)]**, **[USB (Simple)]** and the clients' IPv4 address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.

❒ If you select **[Simple (All)]** or **[Simple (Limitation)]**, you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the printer or if you do not require authentication for printing. However, note that, because the printer does not require authentication in this case, it may be used by unauthorized users.

Reference

For details, see p.39 "Printer Job Authentication Levels and Printer Job Types".

The following procedure is based on **[Entire]** or **[Simple (All)]** being selected.

If you select **[Simple (Limitation)]**, proceed to "Specifying **[Simple (Limitation)]**".

8 Select [Entire] or [Simple (All)].

If global groups have been registered under Windows server, you can limit the use of functions for each global group.

You need to create global groups in the Windows server in advance and register in each group the users to be authenticated.

You also need to register in the printer the functions available to the global group members.

Create global groups in the printer by entering the names of the global groups registered in the Windows Server. (Keep in mind that group names are case sensitive.) Then specify the printer functions available to each group.

If global groups are not specified, users can use the available functions specified in **[Default Group]**. If global groups are specified, users not registered in global groups can use the available functions specified in **[Default Group]**. By default, all functions are available to **[Default Group]** members. Specify the limitation on available functions according to user needs.

9 Click [On] in the "Windows Authentication Settings" area.

10 Enter the domain name to be authenticated.

When you specify the domain name in the Fully Qualified Domain Name format, enter "." at the end of the character string.

11 Enter the group name in the blank area of the "Group Settings for Windows Authentication" box, and then specify the printer functions.

12 Click [OK].

"Updating..." message appears.

13 Click [OK].

Configuration page appears.

14 Quit Web Image Monitor.

Note

❒ Windows Authentication is compatible with NTML v1.

❒ This can also be set using Telnet.

Specifying [Simple (Limitation)]

For authentication, you can also set "Printer Job Authentication" to **[Simple (Limitation)]**.

1. **Select [Simple (Limitation)] in the "Printer Job Authentication" area in the "Printer Job Authentication Settings" area.**

   Specify the range in which **[Simple (Limitation)]** is applied to Printer Job Authentication.

   If you specify IPv4 or IPv6 address range, proceed to step 2.

   If you specify "USB (Simple)", proceed to step 4.

   If you specify "Parallel Interface (Simple)", proceed to step 3.

2. **Select [IPv4 Address 1], [IPv4 Address 2], [IPv4 Address 3], or [IPv4 Address 4], and then enter the IPv4 address on the "Limitation Range (IPv4)" area.**

   Be sure the number you enter for End IPv4 Address is larger than that for Start IPv4 Address.

   If you want to use IPv6, specify the IPv6 address in the "Limitation Range (IPv6)" area.

3. **Click [Apply] in the "Parallel Interface (Simple)" area.**

4. **Click [Apply] in the "USB (Simple)" area.**

5. **Click [OK].**

   "Updating..." message appears.

6. **Click [OK].**

   Configuration page appears.

7. **Quit Web Image Monitor.**

Installing Internet Information Services (IIS) and Certificate services

Specify this setting if you want the printer to automatically obtain e-mail addresses registered in Active Directory.

We recommended you install Internet Information Services (IIS) and Certificate services as the Windows components.

Install the components, and then create the server certificate.

If they are not installed, install them as follows:

① Select **[Add/Remove Programs]** on the **[Control Panel]**.
② Select **[Add/Remove Windows Components]**.
③ Select the **[Internet Information Services (IIS)]** check box.
④ Select the **[Certificate Services]** check box, and then click **[Next >]**.
⑤ Installation of the selected Windows components starts, and a warning message appears.
⑥ Click **[Yes]**.
⑦ Click **[Next >]**.
⑧ Select the Certificate Authority, and then click **[Next >]**.
On the displayed screen, **[Enterprise root CA]** is selected.
⑨ Enter the Certificate Authority name (optional) in **[CA Identifying Information]**, and then click **[Next >]**.
⑩ Leave **[Data Storage Location]** at its default, and then click **[Next]**.

Creating the Server Certificate

After installing Internet Information Services (IIS) and Certificate services Windows components, create the Server Certificate as follows:

① Start **[Internet Services Manager]**.
② Right-click **[Default Web Site]**, and then click **[Properties]**.
③ On the **[Directory Security]** tab, click **[Server Certificate]**.
Web Server Certificate Wizard starts.
④ Click **[Next >]**.
⑤ Select **[Create a new certificate]**, and then click **[Next >]**.
⑥ Select **[Prepare the request now, but send it later]**, and then click **[Next >]**.
⑦ Enter the required information according to the instructions given by Web Server Certificate Wizard.
⑧ Check the specified data, which appears as Request File Summary, and then click **[Next >]**.
The server certificate is created.

Note

❒ After user authentication at the Windows server is set, when logging in using LDAP protocol to obtain name and information to differentiate user at the server, enable SSL communication to prevent information leakage.

LDAP Authentication

Specify this authentication when using the LDAP server to authenticate users who have their accounts on the LDAP server. Users cannot be authenticated if they do not have their accounts on the LDAP server. The address book stored in the LDAP server can be registered to the printer, enabling user authentication without first using the printer to register individual settings in the address book. When using LDAP Authentication, to prevent the password information being sent over the network unencrypted, the printer and LDAP server must communicate via SSL. To enable this, you must create a server certificate for the LDAP server. You can specify on the LDAP server whether or not to enable SSL.

Using Web Image Monitor, you can specify whether or not to check the reliability of the SSL server being connected to.

Important

❒ During LDAP Authentication, the data registered in the LDAP server is automatically registered in the printer. If user information on the server is changed, information registered in the printer may be overwritten when authentication is performed.

❖ **Operational Requirements for LDAP Authentication**

To specify LDAP authentication, the following requirements must be met:

- The optional hard disk
- The network configuration must allow the printer to detect the presence of the LDAP server.
- When SSL is being used, TLSv1, SSLv2, or SSLv3 can function on the LDAP server.
- The LDAP server must be registered in the printer.
  For details about registration, see Software Guide.

Limitation

❒ Under LDAP authentication, you cannot specify access limits for groups registered in the LDAP Server.

❒ When using LDAP Authentication, you cannot use reference functions in LDAP Search for servers using SSL.

❒ Enter the user's login user name using up to 32 characters and login password using up to 128 characters.

❒ Do not use double-byte Japanese, Traditional Chinese, Simplified Chinese, or Hangul characters when entering the login user name or password. If you use double-byte characters, you cannot authenticate using Web Image Monitor.

Note

❒ Under LDAP Authentication, if "Anonymous Authentication" in the LDAP server's settings is not set to "Prohibit", users who do not have an LDAP server account might still be able to gain access.

❒ If the LDAP server is configured using Windows Active Directory, Anonymous Authentication might be available. If Windows Authentication is available, we recommend you use it.

❒ The first time an unregistered user accesses the machine after LDAP authentication has been specified, the user is registered in the printer and can use the functions available under **[Function permissions]** during LDAP Authentication. To limit the available functions for each user, register each user and corresponding **[Function permissions]** setting in the address book, or specify **[Function permissions]** for each registered user. The **[Function permissions]** setting becomes effective when the user accesses the printer subsequently.

Specifying LDAP Authentication

This can be specified by the machine administrator.

Specify the LDAP authentication using Web Image Monitor.

1. **Log on to Web Image Monitor in the administrator mode.**
2. **Click [Configuration].**
3. **Click [Administrator Authentication Management] in the "Device Settings" area.**
4. **Click [On] in the "User Administrator Authentication" area, and then click [OK].**
   Configuration page appears.
5. **Click [User Authentication Management] in the "Device Settings" area.**
6. **Select "LDAP Authentication" in the "User Authentication Management" list.**
   If you do not want to use user authentication management, select **[Off]**.
7. **Select the "Printer Job Authentication" level.**

   Note

   - If you select **[Entire]**, you cannot print using a printer driver or a device that does not support authentication. To print under an environment that does not support authentication, select **[Simple (All)]**.
   - If you select **[Simple (Limitation)]**, you can specify clients for which printer job authentication is not required. Specify "Parallel Interface (Simple)", "USB (Simple)" and the clients' IPv4 or IPv6 address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.
   - If you select **[Simple (All)]** or **[Simple (Limitation)]**, you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the printer or if you do not require authentication for printing. However, note that, because the printer does not require authentication in this case, it may be used by unauthorized users.

   Reference

   For details, see p.39 "Printer Job Authentication Levels and Printer Job Types".

   The following procedure is based on **[Entire]** or **[Simple (All)]** being selected.

   If you select **[Simple (Limitation)]**, proceed to "Specifying **[Simple (Limitation)]**".
8. **Enter the "Login Name Attribute" in the "LDAP Authentication Settings" area.**
   You can use the Login Name Attribute as a search criterion to obtain information about an authenticated user. You can create a search filter based on the Login Name Attribute, select a user, and then retrieve the user information from the LDAP server so it is transferred to the printer's address book. The method for selecting the user name depends on the server environment. Check the server environment and enter the user name accordingly.

9 Enter the "Unique Attribute".

Specify Unique Attribute on the printer to match the user information in the LDAP server with that in the printer. By doing this, if the Unique Attribute of a user registered in the LDAP server matches that of a user registered in the printer, the two instances are treated as referring to the same user. You can enter an attribute such as "serialNumber" or "uid". Additionally, you can enter "cn" or "employeeNumber", provided it is unique. If you do not specify the Unique Attribute, an account with the same user information but with a different login user name will be created in the printer.

10 Click [OK].

"Updating..." message appears.

11 Click [OK].

Configuration page appears.

12 Quit Web Image Monitor.

Note

❒ This can also be set using Telnet.

Specifying Exclusion

For authentication, you can also set **[Print Job Authentication]** to **[Simple (Limitation)]**.

1 Select [Simple (Limitation)] in the "Printer Job Authentication" list in the "Printer Job Authentication Settings" area.

Specify the range in which **[Simple (Limitation)]** is applied to Printer Job Authentication.

If you specify IPv4 or IPv6 address range, proceed to step **2**.

If you specify "USB (Simple)", proceed to step **4**.

If you specify "Parallel Interface (Simple)", proceed to step **3**.

2 Select [IPv4 Address 1], [IPv4 Address 2], [IPv4 Address 3], or [IPv4 Address 4], and then enter the IPv4 address on the "Limitation Range (IPv4)" area.

Be sure the number you enter for End IPv4 Address is larger than that for Start IPv4 Address.

If you want to use IPv6, specify the IPv6 address in the "Limitation Range (IPv6)" area.

3 Click [Apply] in the "Parallel Interface (Simple)" area.

4 Click [Apply] in the "USB (Simple)" area.

5 Click [OK].

Other settings are as same as when you select **[Entire]** or **[Simple (All)]**.

Integration Server Authentication

To use Integration Server Authentication, you need a server on which ScanRouter software that supports authentication is installed.

For external authentication, the Integration Server Authentication collectively authenticates users accessing the server over the network, providing a server-independent centralized user authentication system that is safe and convenient.

To use **[Integration Server Authentication]**, the printer must have access to a server on which the ScanRouter delivery software or Web SmartDeviceMonitor, and **[Authentication Manager]** are installed.

For details about the software, contact your local dealer.

To use Integration Server Authentication, which depends on communication via the secure sockets layer (SSL), the optional hard disk unit must be installed.

Using Web Image Monitor, you can specify whether or not to check the reliability of the SSL server being connected to.

Important

❒ During Integration Server Authentication, the data registered in the server is automatically registered in the printer. If user information on the server is changed, information registered in the printer may be overwritten when authentication is performed.

Note

❒ The built-in default administrator name is "Admin" on the Server and "admin" on the printer.

Specifying Integration Server Authentication

This can be specified by the machine administrator.

This section explains how to specify the printer settings.

For details, see the Authentication Manager manual.

Specify the integration server authentication using Web Image Monitor.

1. **Log on to Web Image Monitor in the administrator mode.**
2. **Click [Configuration].**
3. **Click [Administrator Authentication Management] in the "Device Settings" area.**
4. **Click [On] in the "User Administrator Authentication" area, and then click [OK].**
5. **Click [User Authentication Management] in the"Device Settings" area in the "Configuration" area.**
6. **Select [Integration Server Authentication] in the "User Authentication Management" list.**

   If you do not wish to use User Authentication Management, select **[Off]**.

7 Select the "Printer Job Authentication" level.

Note

❒ If you select **[Entire]**, you cannot print using a printer driver or a device that does not support authentication. To print under an environment that does not support authentication, select **[Simple (All)]**.

❒ If you select **[Simple (Limitation)]**, you can specify clients for which printer job authentication is not required. Specify "Parallel Interface (Simple)", "USB (Simple)" and the clients' IPv4 or IPv6 address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.

❒ If you select **[Simple (All)]** or **[Simple (Limitation)]**, you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the printer or if you do not require authentication for printing. However, note that, because the printer does not require authentication in this case, it may be used by unauthorized users.

Reference

For details, see p.39 "Printer Job Authentication Levels and Printer Job Types".

The following procedure is based on **[Entire]** or **[Simple (All)]** being selected.

If you select **[Simple (Limitation)]**, proceed to "Specifying **[Simple (Limitation)]**".

8 Select [Entire] or [Simple (All)].

9 Click [On] in the "Integration Server Authentication" area.

To not use secure sockets layer (SSL) for authentication, press **[Off]**.

10 Enter the "Integration Server Name".

11 Select "Authentication Type" in the list.

If you set "Authentication Type" to "Windows Authentication (NT Compatible)" or "Windows Authentication (Native)", you can use the global group. If you set "Authentication Type" to "Notes", you can use the Notes group. If you set "Authentication Type" to "Basic Authentication (Integration Server)", you can use the groups created using the Authentication Manager.

12 Enter the "Domain Name".

13 When setting a new group, enter the group name in the blank area of the "Group Settings for Integration Server Authentication" box, and then specify the function.

Note

❒ This can also be set using Telnet.

Specifying Exclusion

For authentication, you can also set **[Print Job Authentication]** to **[Simple (Limitation)]**.

1. **Select [Simple (Limitation)] in the "Printer Job Authentication" list in the "Printer Job Authentication Settings" area.**
   Specify the range in which **[Simple (Limitation)]** is applied to Printer Job Authentication.
   If you specify IPv4 or IPv6 address range, proceed to step 2.
   If you specify "USB (Simple)", proceed to step 4.
   If you specify "Parallel Interface (Simple)", proceed to step 3.

2. **Select [IPv4 Address 1], [IPv4 Address 2], [IPv4 Address 3] or [IPv4 Address 4], and then enter the IPv4 address on the "Limitation Range (IPv4)" area.**
   Be sure the number you enter for End IPv4 Address is larger than that for Start IPv4 Address.
   If you want to use IPv6, specify the IPv6 address in the "Limitation Range (IPv6)" area.

3. **Click [Apply] in the "Parallel Interface (Simple)" area.**

4. **Click [Apply] in the "USB (Simple)" area.**
   Follow the same procedure when you select **[Entire]** or **[Simple (All)]**.

❖ **Printer Job Authentication Levels and Printer Job Types**

This section explains the relationship between printer job authentication levels and printer job types.
Depending on the combination of printer job authentication level and printer job type, the printer may not print properly. Set an appropriate combination according to the operating environment.
User authentication is supported by the RPCS printer driver.

Printer Settings			Printer Job Types						
[User Authentication Management]	[Permit Simple Encryption]	[Simple Encryption]	①	②	③	④	⑤	⑥	⑦
[Off]	—	—	☆	☆	☆	☆	☆	☆	☆
[User Code Authentication],[Basic Authentication], [Windows Authentication],[LDAP Authentication], [Integration Server Authentication]	[Simple]	[Off]	●	❍	×	☆	☆	☆	❍
		[On]		×					
	[Entire]	[Off]	●	❍	×	❍	×	×	❍
		[On]		×					

☆: Printing is possible regardless of user authentication.
❍: Printing is possible if user authentication is successful. If user authentication fails, the print job is reset.
●: Printing is possible if user authentication is successful and **[Driver Encryption Key]** for the printer driver and printer match.
×: Printing is not possible regardless of user authentication, and the print job is reset.

Reference

For details about **[Simple Encryption]**, see p.79 "Changing the Extended Security Functions".

❖ **[Print Job Authentication]**

- **[Entire]**
  The machine authenticates all printer jobs and remote settings, and cancels jobs and settings that fail authentication.
  Printer Jobs: Job Reset
  Settings: Disabled
- **[Simple (All)]**
  The machine authenticates printer jobs and remote settings that have authentication information, and cancels the jobs and settings that fail authentication. Printer jobs and settings without authentication information are performed without being authenticated.
- **[Simple (Limitation)]**.
  You can specify the range to apply **[Simple (Limitation)]** to by specifying "Parallel Interface (Simple)", "USB (Simple)", and the client's IPv4 or IPv6 address.

❖ **Printer Job Types**

① In the RPCS printer driver dialog box, the **[Confirm authentication information when printing]** and **[Encrypt]** check boxes are selected.
Personal authentication information is added to the printer job.
The printer driver applies advanced encryption to the login passwords.
The printer driver encryption key, enables the driver encryption to prevent the login password being stolen.

② In the RPCS printer driver dialog box, the **[Confirm authentication information when printing]** check box is selected.
Personal authentication information is added to the printer job.
The printer driver applies simple encryption to login passwords.

③ In the RPCS printer driver dialog box, the **[Confirm authentication information when printing]** check box is not selected.
Personal authentication information is added to the printer job and is disabled.

④ When using the PostScript 3 printer driver, the printer job contains user code information.
Personal authentication information is not added to the printer job but the user code information is.

Note

❒ This type also applies to recovery/parallel printing using an RPCS printer driver that does not support authentication.

⑤ When using the PostScript 3 printer driver, the printer job does not contain user code information.
Neither personal authentication information nor user code information is added to the printer job.

Note

❒ Type 5 also applies to recovery/parallel printing using an RPCS printer driver that does not support authentication.

⑥ A printer job or PDF file is sent from a host computer without a printer driver and is printed via LPR.
Personal authentication information is not added to the printer job.

⑦ A PDF file is printed via ftp.
Personal authentication is performed using the user ID and password used for logging on via ftp. However, the user ID and password are not encrypted.

Using authfree command (telnet)

Use the "msh> set authfree" command to display and configure authentication exclusion control settings.

❖ **View Settings**

msh> authfree
If print job authentication exclusion is not set, authentication exclusion control cannot be displayed.

❖ **IPv4 address settings**

mah> authfree "ID" range_addr1 range_add2

❖ **IPv6 address settings**

mah> authfree "ID" range6_addr1 range6_add2

❖ **IPv6 address mask settings**

mah> authfree "ID" mask6_addr1 maskln

❖ **Parallel/USB settings**

msh> authfree [parallel|usb] [on|off]
To enable authfree, set to "on". To disable authfree, set to "off".
Always specify the interface.

❖ **Authentication exclusion control initialization**

msh> authfree flush

Note

❒ For IPv4 and IPv6, up to five access ranges can be registered and selected.

If User Authentication Has Been Specified

When user authentication (User Code Authentication, Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication) is set, the authentication screen is displayed. Unless a valid user name and password are entered, operations are not possible with the printer. Log on to operate the printer, and log off when you are finished operations. Be sure to log off to prevent unauthorized users from using the printer. When auto logout timer is specified, the printer automatically logs you off if you do not use the control panel within a given time. Additionally, you can authenticate using an external device.

Note

❒ Consult the User Administrator about your login user name, password, and user code.

❒ For user code authentication, enter a number registered in the address book as **[User Code]**.

User Code Authentication (Using the Control Panel)

When user authentication is set, the following screen appears.

Enter a user code (up to eight digit), and then press the 【Menu】 key.

Note

❒ To log off, do one of the following:

- Press the Operation switch.
- Press the 【Menu】 key, select **[System]**, press the 【OK】 key, and then press the 【Menu】 key again.

User Code Authentication (Using a Printer Driver)

When user authentication is set, specify the user code in the printer properties of a printer driver. For details, see the printer driver Help.

Login (Using the Control Panel)

Follow the procedure below to log on when basic authentication, Windows authentication, LDAP Authentication, or Integration Server Authentication is set.

1. **When the login user name windows appears, press [Text].**
   The window for entering the password appears.
2. **Enter the login user name by pressing the 【▲】【▼】【◄】【►】 and 【OK】keys, and then press [Exit].**
3. **When the message prompting to enter the login password appears, press [Text].**
4. **Enter the login password by pressing the 【▲】【▼】【◄】【►】 and 【OK】keys, and then press [Exit].**
   When the user is authenticated, the screen for the function you are using appears.

Log Off (Using the Control Panel)

Follow the procedure below to log off when Basic Authentication, Windows Authentication, or LDAP Authentication is set.

1. **Press the [Menu] key.**
2. **Press [Logout].**
3. **Press [Yes].**

Login (Using a Printer Driver)

When Basic Authentication, Windows Authentication, or LDAP Authentication is set, make encryption settings in the printer properties of a printer driver, and then specify a login user name and password. For details, see the printer driver Help.

Note

❒ When logged on using a printer driver, logging off is not required.

Login (Using Web Image Monitor)

This section explains how to log onto the printer via Web Image Monitor.

1. **Click [Login].**
2. **Enter a login user name and password, and then click [Login].**

Note

❒ For user code authentication, enter a user code in **[User Name]**, and then click **[OK]**.

❒ The procedure may differ depending on the Web Image Monitor used.

Log Off (Using Web Image Monitor)

1. **Click [Logout] to log off.**

Note

❒ Delete the cache memory in the Web Image Monitor after logging off.

Auto Logout

This can be specified by the machine administrator.

When using user authentication management, the printer automatically logs you off if you do not use the control panel within a given time. This feature is called "Auto Logout". Specify how long the printer is to wait before performing Auto Logout.

1. **Log on to Web Image Monitor in the administrator mode.**
2. **Click [Configuration].**
3. **Click [Timer] in the "Device Settings" area.**
4. **Select [On] in the "Auto Logout" area.**

   Enter "60" to "999" (seconds) using the number keys, and then press **[OK]**.

   Note

   ❒ If you do not want to specify **[Auto Logout Timer]**, select **[Off]**.

5. **Click [OK].**

   Configuration page appears.

6. **Quit Web Image Monitor.**

Authentication using an external device

If you authenticate using an external device, see the Kit manual. For details, contact your local dealer.

3. Preventing Information Leaks

Guarding Against Unauthorized Copying

Using the printer driver, you can embed a pattern in the printed copy to discourage or prevent unauthorized copying.

If you enable data security for copying on the printer, printed copies of a document with data security for copying are grayed out to prevent unauthorized copying.

Make the setting as follows:

❖ Unauthorized Copy Prevention

- Using the printer driver, specify the printer settings for unauthorized copy prevention.
  See p.49 “Specifying Printer Settings for Unauthorized Copy Prevention (Printer Driver Setting)”.

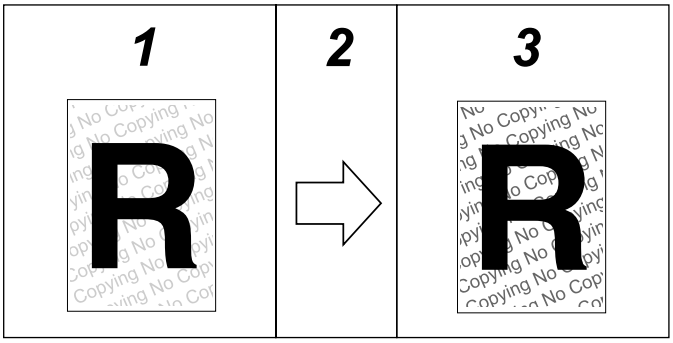
❖ Data security for copying

- Using the printer driver, specify the printer settings for data security for copying.
  See p.49 “Specifying Printer Settings for Data security for copying (Printer Driver Setting)”.

Unauthorized Copy Prevention

Using the printer driver, you can embed mask and pattern (for instance, a warning such as "No Copying") in the printed document.

If the document is copied, scanned, or stored by a copier or multifunction printer, the embedded pattern appears clearly on the copy, discouraging unauthorized copying.



AKB001S

1. Printed Documents

Using the printer driver, you can embed background images and pattern in a printed document for Unauthorized Copy Prevention.

2. The document is copied or scanned.

You cannot store files in this printer.

3. Printed Copies

Embedded pattern (for instance, a warning such as "No Copying") in a printed document appears conspicuously in printed copies.

Important

- ❒ Unauthorized copy prevention discourages unauthorized copying, and will not necessarily stop information leaks.
- ❒ The embedded pattern is not assured to be copied or scanned properly.

Note

- ❒ Depending on the printer settings, the embedded pattern may not be copied or scanned.
- ❒ To make the embedded pattern clear, set the character size to at least 50 pt (preferably 70 to 80 pt) and character angle to between 30 and 40 degrees.

Reference

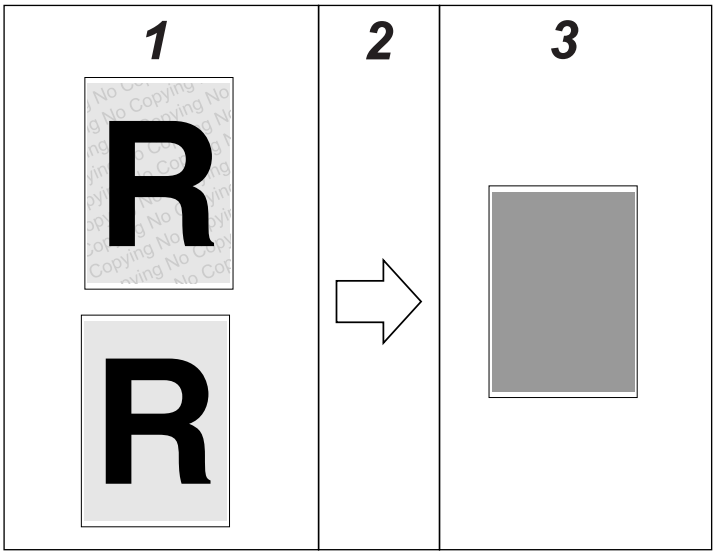
To use the printer function under the User Authentication, you must enter the login user name and password for the printer driver.

For details see the printer driver Help.

Data security for copying

Using the printer driver to enable data security for the copying function, you can print a document with an embedded pattern of hidden text. Such a document is called a data security for copying document.

If a data security for copying document is copied or stored using a copier or multi-function printer that has the Copy Data Security Unit, protected pages are grayed out in the copy, preventing confidential information being copied. Also if a document that has an embedded pattern is detected, the printer beeps. In addition, a log of unauthorized copies is stored. To gray out copies of data security for copying documents when they are copied the optional Copy Data Security Unit must be installed in the supplier's copiers/multifunction machines.



1. **Documents with data security for copying**

2. **The document is copied.**

3. **Printed Copies**

Text and images in the document are grayed out in printed copies.

Note

- ❒ If a document with embedded pattern for data security for copying is copied by a copier or multi-function machine without the supplier's Copy Data Security Unit, the embedded pattern appears conspicuously in the copy. However, how conspicuously the text appears depends on the model of the copier or multi-function printer being used and its scanning setting.
- ❒ You can also embed pattern in a document protected by data security for copying. However, if such a document is copied or stored using a copier or multi-function printer with the Copy Data Security Unit, the copy is grayed out, so the embedded pattern does not appear on the copy.
- ❒ If a document with embedded pattern for data security for copying is copied, scanned, or stored using a copier or multi-function printer without the Copy Data Security Unit, the embedded pattern appears clearly on the copy.

The optional Copy Data Security Unit is for the supplier's copiers/multifunction machines. It cannot be installed on this printer.

Printing Limitations

The following is a list of limitations on printing with unauthorized copy prevention and data security for copying.

❖ **Unauthorized copy prevention / Data security for copying**

Limitation

❒ You can print using the only RPCS printer driver.

❒ You cannot partially embed pattern in the printed document.

❒ You can only embed pattern that is entered in the **[Text:]** box of the printer driver.

❒ Printing with embedding takes longer than normal printing.

❖ **Data security for copying Only**

Limitation

❒ Select 182 × 257 mm / 7.2 × 10.1 inches or larger as the paper size.

❒ Select Plain or Recycled with a brightness of 70% or more as the paper type.

❒ If you select Duplex, the data security for copying function may not work properly due to printing on the back of sheets.

Notice

- The supplier does not guarantee that unauthorized copy prevention and data security for copying will always work. Depending on the paper, the model of copier or multi-function printer, and the copier or printer settings, unauthorized copy prevention and data security for copying may not work properly.
- The supplier is not liable for any damage caused by using or not being able to use unauthorized copy prevention and data security for copying.

Printing with Unauthorized Copy Prevention and Data Security for Copying

Specifying Printer Settings for Unauthorized Copy Prevention (Printer Driver Setting)

Using the printer driver, specify the printer settings for unauthorized copy prevention.

To use the printer function under the User Authentication, you must enter the login user name and password for the printer driver.

For details see the printer driver Help.

For details about specifying data security for copying using the printer driver, see the printer driver Help.

1. **Open the printer driver dialog box.**
2. **On the [Edit] tab, select the [Unauthorized copy...] check box.**
3. **Click [Control Settings...].**
4. **In the [Text:] box in the [Unauthorized copy prevention: Pattern] group, enter the text to be embedded in the printed document.**
   Also, specify **[Font]**, **[Font style:]**, and **[Size]**.
5. **Click [OK].**

Reference

For details, see the printer driver Help.

Specifying Printer Settings for Data security for copying (Printer Driver Setting)

If a document printed using this function is copied or stored in the Document Server by a copier or multi-function printer, the copy is grayed out.

Using the printer driver, specify the printer settings for data security for copying.

For details about data security for copying, see p.47 “Data security for copying”.

To use the printer function under the User Authentication, you must enter the login user name and password for the printer driver.

For details see the printer driver Help.

For details about specifying data security for copying using the printer driver, see the printer driver Help.

1. **Open the printer driver dialog box.**
2. **On the [Edit] tab, select the [Unauthorized copy...] check box.**
3. **Click [Control Settings...].**
4. **In the [Unauthorized copy prevention: Pattern] group, check the [Data security for copying:].**
5. **Click [OK].**

Reference

For details, see the printer driver Help.

Printing a Confidential Document

Depending on the location of the printer, it is difficult to prevent unauthorized persons from viewing prints lying in the printer's output trays. When printing confidential documents, use the Locked Print function.

❖ **Locked Print**

Using the printer's Locked Print function, store files in the printer as Locked Print files and then print them from the control panel and retrieve them immediately, preventing others from viewing them.

Note

❒ To store files temporarily, select **[Stored Print]** under the printer driver. If you select **[Share stored print files]**, also, you can share these files.

❒ When the user authentication is enabled, documents are locked at the time of login, so other printing such as Sample Print, and Hold Print, Stored Print can be safely used. Also, access permits can be enabled on Stored Print using Web Image Monitor.

Choosing a Locked Print file

Using the printer driver, specify a Locked Print file.

If user authentication has been enabled, you must enter the login user name and login password using the printer driver. For details see the printer driver Help.

You can perform Locked Print even if user authentication is not enabled. For details see Software Guide.

1 Open the printer driver dialog box.

2 Set [Job type:] to [Locked Print].

3 Click [Details...].

4 Enter the user ID and password.

The password entered here let you use the Locked Print function.
To print a Locked Print file, enter the same password on the control panel.
Enter the user ID using up to 8 alphanumeric characters.
Enter the password using 4 to 8 numbers.

5 Click [OK].

A confirmation message appears.

6 Confirm the password by re-entering it.

7 Click [OK].

8 Perform Locked Print.

Reference

For details, see the printer driver Help.

Printing a Locked Print File

Print Locked Print files using the control panel.
Consult your administrator if you have forgotten your password.
This can also be specified via Web Image Monitor.
For details see the Web Image Monitor Help.

Preparation

For details about logging on and logging off with user authentication, see p.42 "Login (Using the Control Panel)", p.43 "Log Off (Using the Control Panel)".

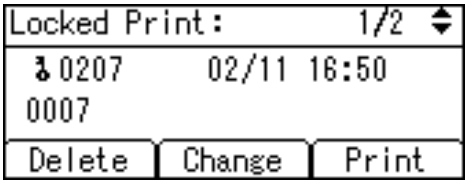
1 **On the printer's control panel, press [Prt.Jobs].**

A list of print files stored in the printer appears.

2 **Select [Locked Print Jobs] using the [▲] or [▼]key, and then press [Job List].**

A list of Locked Print files stored in the printer appears.

3 **Select the file you want to print using the [▲] or [▼] key, and then press [Print].**



The password screen appears.

4 **Enter the password using the [▲]or [▼] key, and then press the [OK] key.**

The print confirmation screen appears.
A confirmation screen will appear if the password is not entered correctly. Press **[Exit]** to enter the password again.
If multiple print files are selected, the printer prints files that correspond to the entered password. The number of files to be printed is displayed on the confirmation screen.

5 **Press [Print].**

Deleting Locked Print Files

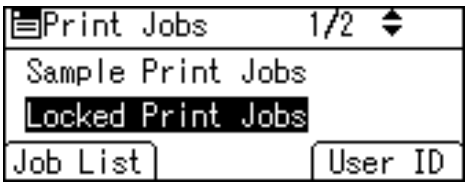
This can be specified by the file creator (owner).
To delete Locked Print files, you must enter the password for the files. If the password has been forgotten, ask the file administrator to change the password.
This can also be specified via Web Image Monitor.
For details see the Web Image Monitor Help.

Note

❒ Locked Print files can also be deleted by the file administrator.

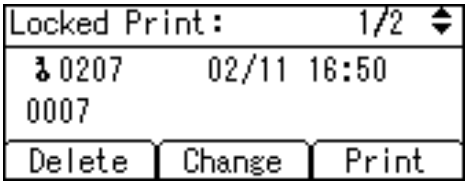
1. **Press [Prt.Jobs].**

2. **Select [Locked Print Jobs] using the [▲] or [▼]key, and then press [Job List].**



A list of Locked Print files stored appears.

3. **Select the file you want to delete using the [▲] or [▼]key, and then press [Delete].**



The password screen is displayed.

4. **Enter the password using the [▲] or [▼] key, and then press the [OK] key.**

The delete confirmation screen appears.
A confirmation screen will appear if the password is not entered correctly. Press **[Exit]** to enter the password again.
If multiple print files are selected, the printer deletes files that correspond to the entered password. The number of files to be printed is displayed on the confirmation screen.

5. **Press [Delete].**
The selected file is deleted.

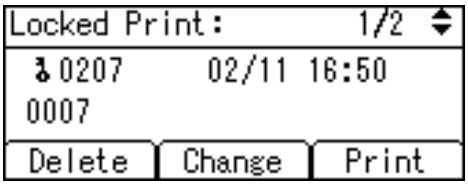
Changing Passwords of Locked Print Files

This can be specified by the file creator (owner) or file administrator.
If the password has been forgotten, the file administrator change the password.
This can also be specified via Web Image Monitor.
For details see the Web Image Monitor Help.

1. **Press [Prt.Jobs].**

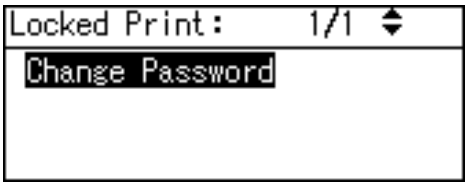
2. **Select [Locked Print Jobs] using the [▲] or [▼]key, and then press [Job List].**

3. **Select the file you want to change the password using the [▲] or [▼] key, and then press [Change].**



4. **Enter the password using the [▲] or [▼] key, and then press the [OK] key.**
   The file administrator does not need to enter the password.

5. **Select [Change Password] using the [▲] or [▼] key, and then press the [OK]key.**



6. **Enter the new password using the [▲] or [▼] key, and then press the [OK] key.**

7. **Re-enter the password, and then press the [OK] key.**

Unlocking Locked Print Files

If you specify "Enhance File Protection", the file will be locked and become inaccessible if an invalid password is entered ten times. This section explains how to unlock files.

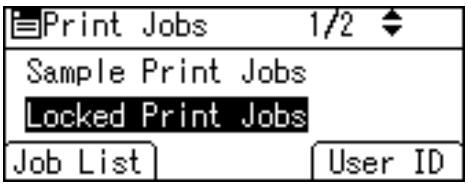
Only the file administrator can unlock files.

This can also be specified via Web Image Monitor. For details see the Web Image Monitor Help.

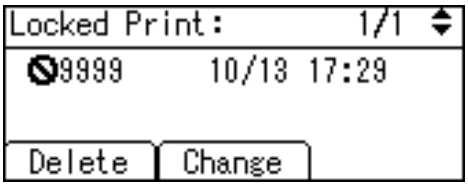
For details about "Enhance File Protection", see p.79 "Changing the Extended Security Functions".

1 **Press [Prt.Jobs].**

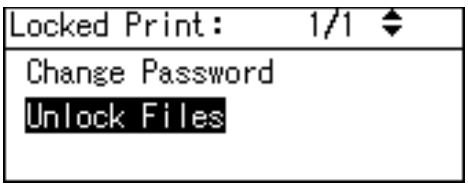
2 **Select [Locked Print Jobs] using the [▲] or [▼]key, and then press [Job List].**



3 **Select the file you want to unlock using the [▲] or [▼] key, and then press [Change].**



4 **Select [Unlock Files] using the [▲] or [▼] key, and then press the [OK] key.**



5 **Press [Unlock].**

Protecting the Address Book

If user authentication is specified, the user who has logged on will be designated as the sender to prevent data from being sent by an unauthorized person masquerading as the user.

To protect the data from unauthorized reading, you can also encrypt the data in the address book.

Address Book Access Permission

This can be specified by the registered user. The access permission can also be specified by a user granted full control or the user administrator.

You can specify who is allowed to access the data in the address book.

By making this setting, you can prevent the data in the address book being used by unregistered users.

1. **Log on to Web Image Monitor in the administrator mode.**
2. **Click [Address Book].**
3. **Click the user you want to specify in the address list, and then click [Change].**

   You can search using Name, Registration No. , or User Code.
4. **Click [Change] in the "Access Privileges" area in the "Protect Destination" area in the "Protection" area.**
5. **Specify the access permission, and then click [OK].**
6. **Click [OK].**

   The **[Address List]** screen appears.
7. **Click [Back].**
8. **Quit Web Image Monitor.**

Encrypting the Data in the Address Book

This can be specified by the user administrator.

Encrypt the data in the address book.

To encrypt the Data in the Address Book, the optional hard disk unit must be installed.

Reference

See p.79 “Changing the Extended Security Functions”.

Preparation

For details about logging on and logging off with administrator authentication, see p.22 “Logging on Using Administrator Authentication”, p.23 “Logging off Using Administrator Authentication”.

Note

❒ If you register additional users after encrypting the data in the address book, those users are also encrypted.

1. **Press the 【Menu】 key.**
2. **Select [Security Options] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
3. **Select [Extended Security] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
4. **Select [Encrypt Address Book] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
5. **Select [On] using the 【▲】 or 【▼】 key, and then press [Enc.Key].**
6. **Enter the encryption key, and then press the 【OK】 key.**

   Enter the encryption key using up to 32 alphanumeric characters.
7. **Re-enter the encryption key, and then press the 【OK】 key.**
8. **Press the 【OK】 key.**
9. **Press [OK].**

   Do not switch the main power off during encryption, as doing so may corrupt the data.

   Encrypting the data in the address book may take a long time.

   The time it takes to encrypt the data in the address book depends on the number of registered users.

   The printer cannot be used during encryption.

   Normally, once encryption is complete, **[Exit]** appears.

   If you press **[Escape]** during encryption, the data is not encrypted.

   If you press **[Escape]** during decryption, the data stays encrypted.
10. **Press [Exit].**
11. **Press the 【Menu】 key.**

4. Managing Access to the Printer

Preventing Modification of printer Settings

Administrator type determines which printer settings can be modified. Users cannot change the administrator settings. In **[Administrator Authentication Management]**, **[Items]**, the administrator can select which settings users cannot specify.

Register the administrators before using the printer.

❖ **Type of Administrator**

Register the administrator on the printer, and then authenticate the administrator using the administrator's login user name and password. The administrator can also specify **[Items]** in **[Administrator Authentication Management]** to prevent users from specifying certain settings. Administrator type determines which printer settings can be modified. The following types of administrator can be designated:

- User Administrator
- Network Administrator
- Machine Administrator
- File Administrator

Reference

For details, see p.13 "Administrators".

For details, see p.19 "Administrator Authentication".

For details, see p.99 "User Administrator Settings".

For details, see p.91 "Machine Administrator Settings".

For details, see p.95 "Network Administrator Settings".

For details, see p.98 "File Administrator Settings".

❖ **Menu Protect**

Use this function to specify the permission level for users to change those settings accessible by non-administrators.

Reference

For details, see p.101 "User Settings".

Menu Protect

The administrator can also limit users' access permission to the printer's settings. The printer's System Settings menu and the printer's regular menus can be locked so they cannot be changed. This function is also effective when management is not based on user authentication.

To change the menu protect setting, you must first enable administrator authentication.

Reference

For details about the menu protect level for each function, see p.101 "User Settings".

Menu Protect

You can set menu protect to **[Off]**, **[Level 1]**, or **[Level 2]**. If you set it to **[Off]**, no menu protect limitation is applied. To limit access to the fullest extent, select **[Level 2]**. For details about the menu protect level for each function, see p.101 "User Settings".

1. **Press the 【Menu】 key.**
2. **Select [Maintenance] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
3. **Select [General Settings] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
4. **Select [Menu Protect] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
5. **Select the menu protect level using the 【▲】 or 【▼】 key, and then press [OK] key.**
6. **Press the 【Menu】 key.**

Limiting Available Functions

To prevent unauthorized operation, you can specify who is allowed to access each of the printer's functions.

Select **[Color/Black&White]** when you want to use both color and black-and-white printing.

Specifying Which Functions are Available

This can be specified by the user administrator. Specify the functions available to registered users. By making this setting, you can limit the functions available to users.

Specify the functions using the Web Image Monitor.

1. **Log on to Web Image Monitor in the administrator mode.**
2. **Click [Address Book].**
3. **Click the user you want to specify in the address list, and then click [Change].**

   You can search using Name, Registration No. , or User Code.
4. **Specify the "Available Functions", and then click [OK].**

   You can select between **[Black&White]** only, or **[Black&White]** and **[Color]**.
5. **Quit Web Image Monitor.**

Managing Log Files

① Log information
To view the log, the log collection server is required.
The following log information is stored in the printer's memory and on its optional hard disk:

- Job log
  Stores information about workflow related to user files.
- Access log
  Stores information about access, such as logging on and off administrator procedures [*1] , and customer engineer procedures. [*2]

[*1] Deleting all log information
[*2] Formatting the optional hard disk

② Deleting log information
To delete the log, the log collection server is required.
By deleting the log stored in the printer, you can free up space on the optional hard disk.

③ Transferring log information
To transfer the log, the log collection server is required.
You can transfer the log information, which indicates who tried to gain access and at what time.
By transferring the log files, you can check the history data and identify unauthorized access.

Specifying Delete All Logs

This can be specified by the machine administrator.

By deleting the log stored in the printer, you can free up space on the optional hard disk.

1 Log on to Web Image Monitor in the administrator mode.

2 Click [Configuration].

3 Click [Logs] in the "Device Settings" area.

4 Click [Delete] in the "Delete All Logs" area.

A confirmation message appears.

5 Press [OK].

6 Press [OK].

7 Quit Web Image Monitor.

Transfer Log Setting

The machine administrator can select **[On]** from the log collection server only.

When using the printer's control panel, you can change the setting to **[Off]** only if it is set to **[On]**.

You can check and change the transfer log setting. This setting lets you transfer log files to the log collection server to check the history data and identify unauthorized access.

For details about log collection server, contact your local dealer.

1. **Press the 【Menu】key.**
2. **Select [Security Options] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
3. **Select [Transfer Log Setting] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
4. **Select [Off] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
5. **Press the 【Menu】key.**

Note

❒ Transfer Log Setting can be set from Web Image Monitor, limitting to Off selection.

Reference

For details about the transfer log setting, see log collection server help.

5. Enhanced Network Security

Preventing Unauthorized Access

You can limit IP addresses, disable ports and protocols, or use Web Image Monitor to specify the network security level to prevent unauthorized access over the network and protect the address book, stored files, and default settings.

Enabling/Disabling Protocols

This can be specified by the network administrator.

Specify whether to enable or disable the function for each protocol.

By making this setting, you can specify which protocols are available and so prevent unauthorized access over the network.

Preparation

For details about logging on and logging off with administrator authentication, see p.22 “Logging on Using Administrator Authentication”, p.23 “Logging off Using Administrator Authentication”.

1. **Press the 【Menu】 key.**
2. **Select [Host Interface] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
3. **Select [Network] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
4. **Select [Effective Protocol] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
5. **Select the protocol you want to specify, and then press the 【OK】 key.**
6. **Select [Invalid] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
7. **Press the 【Menu】 key.**

Reference

Advanced network settings can be specified using Web Image Monitor. For details, see the Web Image Monitor Help.

Access Control

This can be specified by the network administrator.

The printer can control TCP/IP access.

Limit the IP addresses from which access is possible by specifying the access control range.

For example, if you specify the access control range as **[192.168.15.16]**-**[192.168.15.20]**, the client PC addresses from which access is possible will be from 192.168.15.16 to 192.168.15.20.

Limitation

- ❒ Using access control, you can limit access involving LPR, RCP/RSH, FTP, IPP, DIPRINT, Web Image Monitor, SmartDeviceMonitor for Client or DeskTopBinder. You cannot limit the Monitoring of SmartDeviceMonitor for Client.
- ❒ You cannot limit access involving telnet, or SmartDeviceMonitor for Admin.

1 Log on to Web Image Monitor in the administrator mode.

The network administrator can log on using the appropriate login user name and login password.

2 Click [Configuration].

3 Click [Access Control] in the "Security" area.

The **[Access Control]** page appears.

4 To specify the IPv4 Address, in [Access Control Range], enter an IPv4 address that has access to the printer. To specify the IPv6 Address, in [Access Control Range] - [Range], enter an IPv6 address that has access to the printer, or in [Mask], enter an IPv6 address that has access to the printer and specify the [Mask Length].

5 Click [OK].

Access control is set.

6 Quit Web Image Monitor.

Reference

For details, see the Web Image Monitor Help.

Specifying Network Security Level

This can be specified by the network administrator.

This setting lets you change the security level to limit unauthorized access.

Set the security level to **[Level 0]**, **[Level 1]**, or **[Level 2]**.

Select **[Level 2]** for maximum security to protect confidential information.

Select **[Level 1]** for moderate security. Use this setting if the printer is connected to the office local area network (LAN).

Select **[Level 0]** to use this setting if no information needs to be protected.

You can specify the entire network security level setting the printer's control panel.

If you change this setting using Web Image Monitor, the network security level settings other than the specified one will be reset to the default.

Reference

For details about logging on and logging off with user authentication, see p.22 "Logging on Using Administrator Authentication", p.23 "Logging off Using Administrator Authentication".

1 **Press the 【Menu】key.**

2 **Select [Security Options] using the 【▲】or【▼】key, and then press the【OK】key.**

3 **Select [Network Security Level] using the 【▲】or【▼】key, and then press the 【OK】key.**

4 **Select the network security level using the 【▲】or【▼】key, and then press the【OK】key.**

Select **[Level 0]**, **[Level 1]**, or **[Level 2]**.

5 **Press the 【Menu】key.**

Status of Functions under each Network Security Level

❍= Available
— = Unavailable
▲ = Port is open.
△ = Port is closed.
☆ = Automatic
★ = Ciphertext Only
× = Ciphertext Priority

	Function		Network Security Level		
			Level 0	Level 1	Level 2
Interface	Bluetooth		❍	❍	—
TCP/IP	TCP/IP		❍	❍	❍
	HTTP	Port 80	▲	▲	▲
		Port 443	▲	▲	▲

	Function		Network Security Level		
			Level 0	Level 1	Level 2
TCP/IP	HTTP	Port 631	▲	▲	△
		Port 7443/7444	▲	▲	▲
	IPP	Port 80	▲	▲	▲
		Port 631	▲	▲	△
		Port 443	▲	▲	▲
	SSL	Port 443	❍	❍	❍
		SSL / TLS Encryption Mode	×	×	★
	DIPRINT		❍	❍	—
	LPR		❍	❍	—
	FTP	Port 21	▲	▲	▲
	sftp		▲	▲	▲
	ssh	Port 22	▲	▲	▲
	RFU	Port 10021	▲	▲	▲
	RSH/RCP		❍	❍	—
	SNMP		❍	❍	❍
	SNMP v1v2	Setting	❍	❍	—
		Function	❍	❍	—
	SNMP v3		❍	❍	❍
		SNMP Encryption	☆	☆	★
	TELNET		❍	❍	—
	SSDP	Port 1900	▲	▲	△
	NBT	Port 137/138	▲	▲	△
	DNS		❍	❍	—
	SMB		❍	❍	—
NetWare	NetWare		❍	❍	—
AppleTalk	AppleTalk		❍	❍	—

Encrypting Transmitted Passwords

Prevent login passwords, group passwords for PDF files, and IPP authentication passwords being revealed by encrypting them for transmission.

Also, encrypt the login password for administrator authentication and user authentication.

❖ **Driver Encryption Key**

Encrypt the password transmitted when specifying user authentication.
To encrypt the login password, specify the driver encryption key on the printer and on the printer driver installed in the user's computer.

Reference

See p.79 "Changing the Extended Security Functions".

❖ **Group Passwords for PDF Files**

DeskTopBinder Lite's PDF Direct Print function allows a PDF group password to be specified to enhance security.

Note

❒ You cannot perform PDF Direct Print for compressed PDF files.

❖ **Password for IPP Authentication**

To encrypt the IPP Authentication password on the Web Image Monitor, set **[Authentication]** to **[DIGEST]**, and then specify the IPP Authentication password set on the printer.

Note

❒ You can use Telnet or FTP to manage passwords for IPP authentication, although it is not recommended.

Driver Encryption Key

This can be specified by the network administrator.

Specify the driver encryption key on the printer.

By making this setting, you can encrypt login passwords for transmission to prevent them from being analyzed.

Reference

See p.79 “Changing the Extended Security Functions”.

Preparation

For details about logging on and logging off with administrator authentication, see p.22 “Logging on Using Administrator Authentication”, p.23 “Logging off Using Administrator Authentication”.

1. **Press the [Menu] key.**
2. **Select [Security Options] using the [▲] or [▼] key, and then press the [OK] key.**
3. **Select [Extended Security] using the [▲] or [▼] key, and then press the [OK] key.**
4. **Select [Driver Encryption Key] using the [▲] or [▼] key, and then press the [OK] key.**
5. **Enter the driver encryption key, and then press the [OK] key.**

   Enter the driver encryption key using up to 32 alphanumeric characters.

   Note

   ❒ The network administrator must give users the driver encryption key specified on the printer so they can register it on their computers. Make sure to enter the same driver encryption key as that specified on the printer.

6. **Re-enter the driver encryption key, and then press the [OK] key.**
7. **Press the [Menu] key.**

Reference

See the printer driver Help.

Group Password for PDF files

This can be specified by the network administrator.

On the printer, specify the group password for PDF files.

By using a PDF group password, you can enhance security and so protect passwords from being analyzed.

Preparation

For details about logging on and logging off with administrator authentication, see p.22 “Logging on Using Administrator Authentication”, p.23 “Logging off Using Administrator Authentication”.

Note

- ❒ The network administrator must give users the group password for PDF files that is already registered on the printer. The users can then register it in DeskTopBinder on their computers. For details, see the DeskTopBinder Help
- ❒ Make sure to enter the same character string as that specified on the printer for the group password for PDF files.
- ❒ The group password for PDF files can also be specified using Web Image Monitor. For details, see the Web Image Monitor Help.

1 **Press the 【Menu】 key.**

2 **Select [Print Settings] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**

3 **Select [PDF Menu] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**

4 **Select [PDF Group Password] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**

5 **Enter the current password, and then press the [Exit] key.**

Enter the group password for PDF files using up to 32 alphanumeric characters.

6 **Enter the new password, and then press the [Exit] key.**

7 **Re-enter the new password, and then press the [Exit] key.**

8 **Press the 【Menu】 key.**

IPP Authentication Password

This can be specified by the network administrator.

Specify the IPP authentication passwords for the printer using Web Image Monitor.

By making this setting, you can encrypt IPP authentication passwords for transmission to prevent them from being analyzed.

Note

❒ When using the IPP port under Windows XP or Windows Server 2003, you can use the operating system's standard IPP port.

1. **Log on to Web Image Monitor in the administrator mode.**
2. **Click [Configuration].**
3. **Click [IPP Authentication] in the "Security" area.**
   The **[IPP Authentication]** page appears.
4. **Select [DIGEST] from the Authentication list.**
5. **Enter the user name in the [User Name] box.**
6. **Enter the password in the [Password] box.**
7. **Click [OK].**
   IPP authentication is specified.
8. **Quit Web Image Monitor.**

Protection Using Encryption

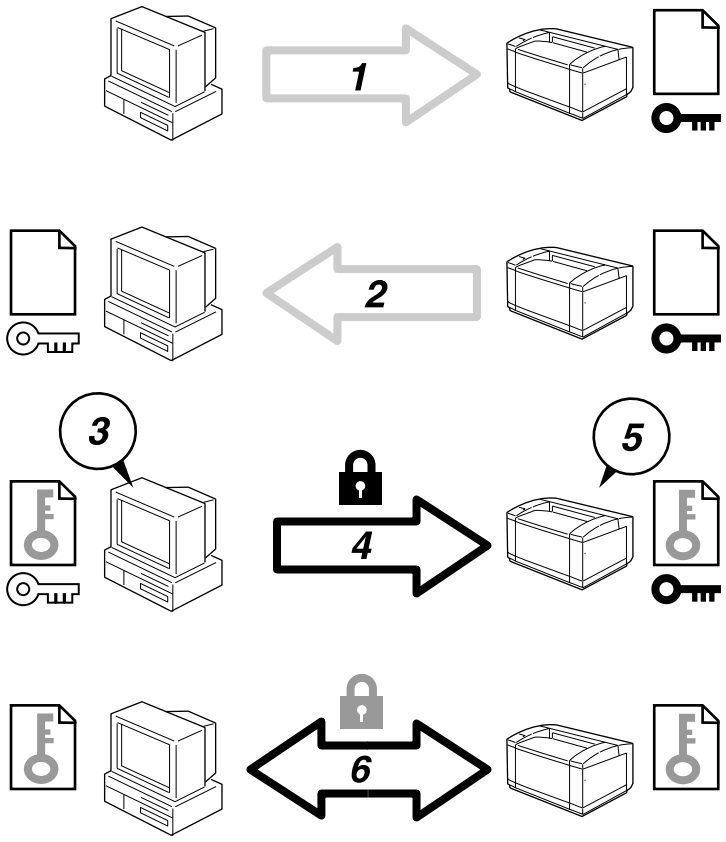
When you access the printer using a Web Image Monitor or IPP, you can establish encrypted communication using SSL. When you access the printer using an application such as SmartDeviceMonitor for Admin, you can establish encrypted communication using SNMPv3 or SSL.

To protect data from interception, analysis, and tampering, you can install a server certificate in the printer, negotiate a secure connection, and encrypt transmitted data.

Important

❒ When using SSL, the optional hard disk or the data storage card are required.

❖ **SSL (Secure Sockets Layer)**



① To access the printer from a user's computer, request for the SSL server certificate and public key.
② The server certificate and public key are sent from the printer to the user's computer.
③ Create shared key from the user's computer, and then encrypt it using public key.
④ The encrypted shared key is sent to the printer.
⑤ The encrypted shared key is decrypted in the machine using private key.
⑥ Transmit the encrypted data using the shared key, and then decrypt the data at the machine to attain secure transmission.

SSL (Secure Sockets Layer) Encryption

This can be specified by the network administrator.

To protect the communication path and establish encrypted communication, create and install the server certificate.

There are two ways of installing a server certificate: create and install a self-certificate using the printer, or request a certificate from a certificate authority and install it.

❖ Configuration flow (self-signed certificate)

① Creating and installing the server certificate
Install the server certificate using Web Image Monitor.

② Enabling SSL
Enable the **[SSL/TLS]** setting using Web Image Monitor.

❖ Configuration flow (certificate issued by a certificate authority)

① Creating the server certificate
Create the server certificate using Web Image Monitor.
The application procedure after creating the certificate depends on the certificate authority. Follow the procedure specified by the certificate authority.

② Installing the server certificate
Install the server certificate using Web Image Monitor.

③ Enabling SSL
Enable the **[SSL/TLS]** setting using Web Image Monitor.
Creating and Installing the Server Certificate (Self-Signed Certificate)
Create and install the server certificate using Web Image Monitor.

Note

❒ To confirm whether SSL configuration is enabled, enter https://(printer's-address) in your Web Image Monitor's address bar to access this printer. If the "The page cannot be displayed" message appears, check the configuration as the SSL configuration is invalid.

Creating and Installing the Self-Signed Certificate

Create and install the server certificate using Web Image Monitor.

This section explains the use of a self-certificate as the server certificate.

1 Log on to Web Image Monitor in the administrator mode.

2 Click [Configuration], and then click [Device Certificate] in the "Security" area..

3 Click [Create].

4 Make the necessary settings.

5 Click [OK].
The setting is changed.

6 Click [OK].
A security warning dialog box appears.

7 **Check the details, and then click [OK].**

[Installed] appears under **[Certificate Status]** to show that a server certificate for the printer has been installed.

8 **Quite Web Image Monitor.**

Note

❒ Click **[Delete]** to delete the server certificate from the printer.

Reference

For details about the displayed items and selectable items, see Web Image Monitor Help.

Creating the Server Certificate (Certificate Issued by a Certificate Authority)

Create the server certificate using Web Image Monitor.

This section explains the use of a certificate issued by a certificate authority as the server certificate.

1 **Log on to Web Image Monitor in the administrator mode.**

2 **Click [Configuration], and then click [Device Certificate] in the "Security" area.**

The **[Device Certificate]** page appears.

3 **Click [Request].**

4 **Make the necessary settings.**

5 **Click [OK].**

[Requesting] appears for **[Certificate Status]** in the **[Device Certificate]** area.

6 **Quite Web Image Monitor.**

7 **Apply to the certificate authority for the server certificate.**

The application procedure depends on the certificate authority. For details, contact the certificate authority.

Note

❒ If you apply for two certificates simultaneously, the certificate authority may not appear in the certificates. When you install these certificates, be sure to take notes of the certificate contents and the order in which the certificates were installed.

❒ Using Web Image Monitor, you can create the contents of the server certificate but you cannot send the application.

❒ Click **[Cancel Request]** to cancel the request for the server certificate.

Reference

For details about the displayed items and selectable items, see Web Image Monitor Help.

Installing the Server Certificate (Certificate Issued by a Certificate Authority)

Install the server certificate using Web Image Monitor.

This section explains the use of a certificate issued by a certificate authority as the server certificate.

Enter the server certificate contents issued by the certificate authority.

1. **Log on to Web Image Monitor in the administrator mode.**
2. **Click [Configuration], and then click [Device Certificate] in the "Security" area.**
   The **[Device Certificate]** page appears.
3. **Click [Install].**
4. **Enter the contents of the server certificate.**
   In the Device Certificate Request box, enter the contents of the server certificate received from the certificate authority.
5. **Click [OK].**
   [Installed] appears under **[Certificate Status]** to show that a server certificate for the printer has been installed.
6. **Quite Web Image Monitor.**

Reference

For details about the displayed items and selectable items, see Web Image Monitor Help.

Enabling SSL

After installing the server certificate in the printer, enable the SSL setting.

This procedure is used for a self-signed certificate or a certificate issued by a certificate authority.

1. **Log on to Web Image Monitor in the administrator mode.**
2. **Click [Configuration], and then click [SSL/TLS] in the "Security" area.**
   The **[SSL/TLS]** page appears.
3. **Click [Enable] for [SSL/TLS].**
4. **Click [OK].**
   The SSL setting is enabled.
5. **Quite Web Image Monitor.**

Note

❒ If you set **[Permit SSL/TLS Communication]** to **[Ciphertext Priority]**, enter "https://(printer's address)/" to access the printer.

User Settings for SSL (Secure Sockets Layer)

If you have installed a server certificate and enabled SSL (Secure Sockets Layer), you need to install the certificate on the user's computer.

The network administrator must explain the procedure for installing the certificate to users.

If a warning dialog box appears while accessing the printer using the Web Image Monitor or IPP, start the Certificate Import Wizard and install a certificate.

1 When the [Security Alert] dialog box appears, click [View Certificate].

The **[Certificate]** dialog box appears.

To be able to respond to inquiries from users about such problems as expiry of the certificate, check the contents of the certificate.

2 On the [General] tab, click [Install Certificate...].

Certificate Import Wizard starts.

3 Install the certificate by following the Certificate Import Wizard instructions.

Note

❒ For details about how to install the certificate, see the Web Image Monitor Help.

❒ If a certificate issued by a certificate authority is installed in the printer, confirm the certificate store location with the certificate authority.

Reference

For details about where to store the certificate when accessing the printer using IPP, see the SmartDeviceMonitor for Client Help.

Setting the SSL / TLS Encryption Mode

By specifying the SSL/TLS encrypted communication mode, you can change the security level.

❖ **Encrypted Communication Mode**

Using the encrypted communication mode, you can specify encrypted communication.

Ciphertext Only	Allows encrypted communication only. If encryption is not possible, the printer does not communicate.
Ciphertext Priority	Performs encrypted communication if encryption is possible. If encryption is not possible, the printer communicates without it.
Ciphertext/Clear Text	Communicates with or without encryption, according to the setting.

Setting the SSL / TLS Encryption Mode

This can be specified by the network administrator.

After installing the server certificate, specify the SSL/TLS encrypted communication mode. By making this setting, you can change the security level.

Specify the SSL/TLS encrypted communication mode using Web Image Monitor.

1. **Log on to Web Image Monitor in the administrator mode.**
2. **Click [Configuration].**
3. **Click [SSL/TLS] in the "Security" area.**
4. **Select the encryption communication mode in the "Permit SSL/TLS Communication" list, and then click [OK].**

   Select **[Ciphertext Only]**, **[Ciphertext Priority]**, or **[Ciphertext/Clear Text]** as the encrypted communication mode.
5. **Quit Web Image Monitor.**

SNMPv3 Encryption

This can be specified by the network administrator.

When using SmartDeviceMonitor for Admin or another application to make various settings, you can encrypt the data transmitted.

By making this setting, you can protect data from being tampered with.

Specify the SNMPv3 encrypted communication mode using Web Image Monitor.

1. **Log on to Web Image Monitor in the administrator mode.**
2. **Click [Configuration].**
3. **Click [Network Security] in the "Security" area.**
4. **Click [Encryption Only] in the "Permit SNMPv3 Communication" area in the "SNMP" area, and then click [OK].**
5. **Quit Web Image Monitor.**

Note

- To use SmartDeviceMonitor for Admin for encrypting the data for specifying settings, you need to specify the network administrator's **[Encryption Password]** setting and **[Encryption Key:]** in **[SNMP Authentication Information]** in SmartDeviceMonitor for Admin, in addition to specifying **[Permit SNMPv3 Communication]** on the printer.
- If network administrator's **[Encryption Password]** setting is not specified, the data for transmission may not be encrypted or sent.

Reference

For details about specifying the network administrator's **[Encryption Password]** setting, see p.21 "Registering the Administrator".

For details about specifying **[Encryption Key:]** in SmartDeviceMonitor for Admin, see the SmartDeviceMonitor for Admin Help.

6. Specifying the Extended Security Functions

Changing the Extended Security Functions

As well as providing basic security through user authentication and the printer access limits specified by the administrators, you can increase security by, for instance, encrypting transmitted data and data in the address book. If you need extended security, specify the printer's extended security functions before using the printer.

This section outlines the extended security functions and how to specify them. For details about when to use each function, see the corresponding chapters.

Changing the Extended Security Functions

To change the extended security functions, display the extended security screen as follows:

Preparation

For details about logging on and logging off with administrator authentication, see p.22 "Logging on Using Administrator Authentication", p.23 "Logging off Using Administrator Authentication".

Procedure for Changing the Extended Security Functions

1. **Press the [Menu] key.**
2. **Select [Security Options] using the [▲] or [▼] key, and then press the [OK] key.**
3. **Select [Extended Security] using the [▲] or [▼] key, and then press the [OK] key.**
4. **Select the setting you want to change using the [▲] or [▼] key, and then press the [OK] key.**
5. **Change the setting, and then press the [OK] key.**
6. **Press the [Menu] key.**

Settings

❖ **Driver Encryption Key**

This can be specified by the network administrator. Encrypt the password transmitted when specifying user authentication. The Driver Encryption Key must match the encryption key set on the printer.

Reference

See the printer driver Help.

❖ **Encrypt Address Book**

This can be specified by the user administrator. Encrypt the data in the printer's address book.

Reference

See p.56 "Encrypting the Data in the Address Book".

- On
- Off

Note

❒ Default: *Off*

❖ **Enhance File Protection**

This can be specified by the file administrator. By specifying a password, you can limit operations such as printing and deleting, and can prevent unauthorized people from accessing the files. However, it is still possible for the password to be cracked.

By specifying "Enhance File Protection", files are locked and so become inaccessible if an invalid password is entered ten times. This can protect the files from unauthorized access attempts in which a password is repeatedly guessed.

The locked files can only be unlocked by the file administrator.

Note

❒ If files are locked, you cannot select them even if the correct password is entered.

- On
- Off

Note

❒ Default: *Off*

❖ **Settings by SNMP v1 and v2**

This can be specified by the network administrator. When the printer is accessed using the SNMPv1, v2 protocol, authentication cannot be performed, allowing machine administrator settings such as the paper setting to be changed. If you select **[Prohibit]**, the setting can be viewed but not specified with SNMPv1, v2.

- On
- Off

Note

❒ Default: *Off*

❖ **Simple Encryption**

This can be specified by the network administrator.
For example, this setting is set to **[On]** and you want to edit the address book in User Management Tool or Address Management Tool in SmartDeviceMonitor for Admin, or you want to access the printer using DeskTopBinder or the ScanRouter delivery software, enable SSL/TLS for encrypted communication. For details about specifying SSL/TLS, see p.76 "Setting the SSL / TLS Encryption Mode".
If you select **[Restrict]**, specify the encryption setting using the printer driver.

- Restrict
- Do not Restrict

Note

❒ Default: *Do not Restrict*

❖ **Authenticate Current Job**

This can be specified by the machine administrator.
This setting lets you specify whether or not authentication is required for operations such as canceling jobs under the printer.
If you select **[Login Privilege]**, authorized users and the machine administrator can operate the printer. When this is selected, authentication is not required for users who logged on to the printer before **[Login Privilege]** was selected. If you select **[Access Privilege]**, users who canceled a print job in progress and the machine administrator can operate the printer.

- Login Privilege
- Access Privilege
- Off

Note

❒ Default: *Off*

❒ Even if you select **[Login Privilege]** and log onto the printer, you cannot cancel a print job in progress if you are not authorized to use the printer.

❒ You can specify **[Authenticate Current Job]** only if **[User Authentication Management]** was specified.

❖ **Password Policy**

This can be specified by the user administrator.

The password policy setting is effective only if **[Basic Authentication]** is specified. This setting lets you specify **[Complexity Setting]** and **[Minimum Character No.]** for the password. By making this setting, you can limit the available passwords to only those that meet the conditions specified in **[Complexity Setting]** and **[Minimum Character No.]**.

If you select **[Level 1]**, specify the password using a combination of two types of characters selected from upper-case letters, lower-case letters, decimal numbers, and symbols such as #.

If you select **[Level 2]**, specify the password using a combination of three types of characters selected from upper-case letters, lower-case letters, decimal numbers, and symbols such as #.

❖ **@Remote Service**

Communication via HTTPS for @Remote Service is disabled if you select **[On]**. When you select **[On]**, contact your service representative.

- On
- Off

Note

❒ Default: *Off*

Limiting Printer Operation to Customers Only

The printer can be set so that operation is impossible without administrator authentication.

The printer can be set to prohibit operation without administrator authentication and also prohibit remote registration in the address book by a service representative.

We maintain strict security when handling customers' data. Also, by being authenticated by an administrator to use the printer, we operate the printer under the customer's control.

Use the following settings.

- Service Mode Lock

Settings

❖ **Service Mode Lock**

This can be specified by the machine administrator. Service mode is used by a customer engineer for inspection or repair. If you set the service mode lock to **[On]**, service mode cannot be used unless the machine administrator logs onto the printer and cancels the service mode lock to allow the customer engineer to operate the printer for inspection and repair. This ensures that the inspection and repair are done under the supervision of the machine administrator.

Specifying Service Mode Lock

Preparation

For details about logging on and logging off with administrator authentication, see p.22 "Logging on Using Administrator Authentication", p.23 "Logging off Using Administrator Authentication".

1. **Press the 【Menu】 key.**
2. **Select [Security Options] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
3. **Select [Service Mode Lock] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
4. **Select [On] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**

   A confirmation message appears.
5. **Press [Yes].**
6. **Press the 【Menu】 key.**

Canceling Service Mode Lock

For a customer engineer to carry out inspection or repair in service mode, the machine administrator must log onto the printer and cancel the service mode lock.

Preparation

For details about logging on and logging off with administrator authentication, see p.22 “Logging on Using Administrator Authentication”, p.23 “Logging off Using Administrator Authentication”.

1. **Press the 【Menu】 key.**
2. **Select [Security Options] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
3. **Select [Service Mode Lock] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
4. **Select [Off] using the 【▲】 or 【▼】 key, and then press the 【OK】 key.**
5. **Press the 【Menu】 key.**

   The customer engineer can switch to service mode.

Authentication Does Not Work Properly

This section explains what to do if a user cannot operate the printer because of a problem related to user authentication. Refer to this section if a user comes to you with such a problem.

A Message Appears

This section explains how to deal with problems if a message appears on the screen during user authentication.

The most common messages are explained. If some other message appears, deal with the problem according to the information contained in the message.

Messages	Causes	Solutions
`You do not have privileges to use this function.`	The authority to use the function is not specified.	• If this appears when trying to use a function: The function is not specified in the address book management setting as being available. The user administrator must decide whether to authorize use of the function and then assign the authority. • If this appears when trying to specify a default setting: The administrator differs depending on the default settings you wish to specify. Using the list of settings, the administrator responsible must decide whether to authorize use of the function.
`Failed to obtain URL.`	The printer cannot connect to the server or cannot establish communication.	Make sure the server's settings, such as the IP Address and host name, are specified correctly on the printer. Make sure the host name of the UA Server is specified correctly.
	The printer is connected to the server, but the UA service is not responding properly.	Make sure the UA service is specified correctly.
	SSL is not specified correctly on the server.	Specify SSL using Authentication Manager.
	Server authentication failed.	Make sure server authentication is specified correctly on the printer.

Messages	Causes	Solutions
Authentication has failed.	The entered login user name or login password is not correct	Inquire the user administrator for the correct login user name and login password.
	The number of users registered in the address book has reached the maximum limit allowed by Windows Authentication or , LDAP Authentication, or Integration Server Authentication, so you cannot register additional users.	Delete unnecessary user addresses.
	Cannot access the authentication server when using Windows authentication , LDAP Authentication, or Integration Server Authentication.	A network or server error may have occurred. Contact to the network administrator.
The selected file(s) contained file(s) without access privileges. Only file(s) with access privileges will be deleted.	You have tried to delete files without the authority to do so.	Files can be deleted by the file creator (owner) or file administrator. To delete a file which you are not authorized to delete, contact the file creator (owner).

Printer Cannot Be Operated

If the following conditions arise while users are operating the printer, provide instructions on how to deal with them.

Condition	Cause	Solution
After starting **[User Management Tool]** or **[Address Management Tool]** in SmartDeviceMonitor for Admin and entering the correct login user name and password, a message appears to notify that an incorrect password has been entered.	"Restrict Simple Encryption" is not set correctly. Alternatively, **[SSL/TLS]** has been enabled although the required certificate is not installed in the computer.	Set "Restrict Simple Encryption" to **[On]**. Alternatively, enable **[SSL/TLS]**, install the server certificate in the printer, and then install the certificate in the computer. **Reference** See p.81 "Simple Encryption". See p.76 "Setting the SSL / TLS Encryption Mode".
Stored files do not appear.	User authentication may have been disabled while **[All Users]** is not specified.	Re-enable user authentication, and then enable **[All Users]** for the files that did not appear. For details about enabling **[All Users]**, see p.55 "Protecting the Address Book"
Destinations specified using the printer do not appear.	User authentication may have been disabled while **[All Users]** is not specified.	Re-enable user authentication, and then enable **[All Users]** for the destinations that did not appear. For details about enabling **[All Users]**, see p.55 "Protecting the Address Book".
Cannot print when user authentication has been specified.	User authentication may not be specified in the printer driver.	Specify user authentication in the printer driver. For details, see the printer driver Help.
After you execute **[Encrypt Address Book]** the **[Exit]** message does not appear.	The optional hard disk may be faulty. The file may be corrupt.	Contact your service representative.

Operations by the Supervisor

The supervisor can delete an administrator's password and specify a new one. If any of the administrators forget their passwords or if any of the administrators change, the supervisor can assign a new password. If logged on using the supervisor's user name and password, you cannot use normal functions or specify defaults. Log on as the supervisor only to change an administrator's password.

Important

- ❒ The default login user name is "supervisor" and the login password is blank. We recommend changing the login user name and login password.
- ❒ When registering login user names and login passwords, you can specify up to 32 alphanumeric characters and symbols. Keep in mind that user names and passwords are case-sensitive.
- ❒ Be sure not to forget the supervisor login user name and login password. If you do forget them, a service representative will to have to return the printer to its default state. This will result in all data in the printer being lost and the service call may not be free of charge.

Note

- ❒ You cannot specify the same login user name for the supervisor and the administrators.

Logging on as the Supervisor

If administrator authentication has been specified, log on using the supervisor login user name and login password. This section describes how to log on.

1. **Start your web browser.**
2. **Enter "http://(printer's Address)/" in the address bar of a Web browser.**

   Top Page of Web Image Monitor appears.
3. **Click [Login].**

   The windows for entering the login user name and password for the Web Image Monitor administrator appears.
4. **Enter the login user name and password, and then click [Login].**

   When you assign the administrator for the first time, enter "supervisor", and leave the password blank.

Logging off as the Supervisor

If administrator authentication has been specified, be sure to log off after completing settings. This section explains how to log off after completing settings.

1. **Click [Logout].**
2. **Quite Web Image Monitor.**

Changing the Supervisor

1. **Log on to Web Image Monitor in the supervisor mode.**
2. **Click [Configuration].**
3. **Click [Program/Change Administrator] in the "Device Settings" area.**
4. **Enter the "Login User Name" in the "Supervisor" box.**
5. **Click [Change] in the "Login Password" area.**
6. **Enter the password, and then click [OK].**
7. **Quit Web Image Monitor.**

Resetting an Administrator's Password

1. **Log on to Web Image Monitor in the supervisor mode.**
2. **Click [Configuration].**
3. **Click [Program/Change Administrator] in the "Device Settings" area.**
4. **Select the Administrator whose password you want to change.**
5. **Click [Change] in the "Login Password" area.**
6. **Enter the password, and then click [OK].**
7. **Quit Web Image Monitor.**

Machine Administrator Settings

The machine administrator settings that can be specified are as follows:

Control Panel

❖ **Paper Input**
All the settings can be specified.

❖ **Maintenance**

- Quality Maintenance
  All the settings can be specified.
- General Settings
  All the settings can be specified.
- Timer Settings
  All the settings can be specified.

❖ **List/Test Print**
All the settings can be specified.

❖ **System**
All the settings can be specified.

❖ **Print Settings**
All the settings can be specified.

❖ **Security Options**

- Extended Security
  Restrict User Info.Display
  Authenticate Current Job
  @Remote Service
- Service Mode Lock
- Transfer Log Setting

❖ **Host Interface**

- I/O Buffer
- I/O Timeout
- IEEE 802.11b
- USB Setting

Settings via Web Image Monitor

The following settings can be specified.

❖ Home Page

- Reset Printer Job
- Reset Device

❖ Device Settings

- System
  Protect Printer Display Panel
  Display Panel Language
  Permit ROM Update
  Display IP Address on Device Display Panel
- Paper
  All the settings can be specified.
- Date/Time
  All the settings can be specified.
- Timer
  All the settings can be specified.
- Logs
  Collect Job Logs
  Collect Access Logs
- E-mail
  - Administrator E-mail Address
  - Reception Protocol
  - SMTP Authentication
  - SMTP Auth. E-mail Address
  - SMTP Auth. User Name
  - SMTP Auth. Password
  - SMTP Auth. Encryption
  - POP before SMTP
  - POP E-mail Address
  - POP User Name
  - POP Password
  - Timeout setting after POP Auth.
  - POP3/IMAP4 Server Name
  - POP3/IMAP4 Encryption
  - E-mail Notification E-mail Address
  - Receive E-mail Notification
  - E-mail Notification User Name
  - E-mail Notification Password
- Auto E-mail Notification
  All the settings can be specified.

- On-demand E-mail Notification
  All the settings can be specified.
- User Authentication Management
  All the settings can be specified.
- Administrator Authentication Management
  Machine Administrator Authentication
  Available Settings for Machine Administrator
- Program/Change Administrator
  You can specify the following administrator settings as the machine administrator.
  Login User Name
  Login Password
  Change Encryption Password
- LDAP Server
  All the settings can be specified.
- ROM Update
  All the settings can be specified.

❖ **Printer**

- Basic Settings
  All the settings can be specified.
- Tray Parameters (PCL)
  All the settings can be specified.
- Tray Parameters (PS)
  All the settings can be specified.
- PDF Group Password
  All the settings can be specified.
- PDF Fixed Password
  All the settings can be specified.

❖ **Interface**

- Parallel Interface
- USB
- PictBridge

❖ **Network**

- SNMPv3

❖ **RC Gate**

All the settings can be specified.

❖ **Security Options**

All the settings can be specified.

❖ **Webpage**

Download Help File

Settings via SmartDeviceMonitor for Admin

The following settings can be specified.

❖ **Device Information**

- Reset Device
- Reset Current Job
- Reset All Jobs

❖ **User Management Tool**

The following settings can be specified.

- User Page Count
- Access Control List
- Reset User Counters

Network Administrator Settings

The network administrator settings that can be specified are as follows:

Control Panel

The following settings can be specified.

❖ Security Options

- Extended Security
  Driver Encryption Key
  Enhance File Protection
  Settings by SNMPv1 and v2
  Simple Encryption
- Network Security Level

❖ Host Interface

- Network
  All the settings can be specified.
- IEEE 802.11b [*1]
  All the settings can be specified.

[*1] The IEEE802.11b interface unit option must be installed.

Settings via Web Image Monitor

The following settings can be specified.

❖ Device Settings

- System
  Device Name
  Comment
  Location
  Display Panel Language
- E-mail
  SMTP
  E-mail Communication Port
- Administrator Authentication Management
  Network Administrator Authentication
  Available Settings for Network Administrator
- Program/Change Administrator
  You can specify the following administrator settings for the machine administrator.
  Login User Name
  Login Password
  Change Encryption Password

❖ Network

- IPv4
  All the settings can be specified.
- IPv6
  All the settings can be specified.
- NetWare
  All the settings can be specified.
- AppleTalk
  All the settings can be specified.
- SMB
  Workgroup Name
  Computer Name
  Comment
  Notify Print Completion
- SNMP
  All the settings can be specified.
- SNMPv3
  All the settings can be specified.
- SSDP
  SSDP
  Profile Expires
  TTL
- Bonjour
  All the settings can be specified.

❖ Security

- Network Security
  All the settings can be specified.
- Access Control
  All the settings can be specified.
- IPP Authentication
  All the settings can be specified.
- SSL/TLS
  All the settings can be specified.
- Site Certificate
  All the settings can be specified.
- Device Certificate
  All the settings can be specified.

❖ Webpage

All the settings can be specified.

Settings via SmartDeviceMonitor for Admin

The following settings can be specified.

❖ **NIB Setup Tool**
All the settings can be specified.

File Administrator Settings

The file administrator settings that can be specified are as follows:

Control Panel

The following settings can be specified.

❖ **Maintenance**
All the settings can be specified.

❖ **Security Options**

- Extended Security
  Enhance File Protection

Settings via Web Image Monitor

The following settings can be specified.

❖ **Device Settings**

- System
  Display Panel Language
- Administrator Authentication Management
  File Administrator Authentication
  Available Settings for File Administrator
- Program/Change Administrator
  You can specify the following administrator settings for the file administrator.
  Login User Name
  Login Password
  Change Encryption Password

❖ **Printer**

- Auto Delete Temporary Print Jobs
- Auto Delete Stored Print Jobs

❖ **Webpage**

- Download Help File

User Administrator Settings

The user administrator settings that can be specified are as follows:

Control Panel

The following settings can be specified.

❖ **Security Options**
- Extended Security
  Encrypt Address Book
  Password Policy

Settings via Web Image Monitor

The following settings can be specified.

❖ **Address Book**
All the settings can be specified.

❖ **Device Settings**
- System
  Display Panel Language
- Auto E-mail Notification
  Group to Notify
- Administrator Authentication Management
  File Administrator Authentication
  Available Settings for File Administrator
- Program/Change Administrator
  The user administrator settings that can be specified are as follows:
  Login User Name
  Login Password
  Change Encryption Password

❖ **Webpage**
- Download Help File

Settings via SmartDeviceMonitor for Admin

The following settings can be specified.

❖ **Address Management Tool**
All the settings can be specified.

❖ **User Management Tool**
- Restrict Access To Device
- Add New User
- Delete User
- User Properties

The Privilege for User Account Settings in the Address Book

The authorities for using the address book are as follows:

The authority designations in the list indicate users with the following authorities.

- Read-only
  This is a user assigned "Read-only" authority.
- Edit
  This is a user assigned "Edit" authority.
- Edit / Delete
  This is a user assigned "Edit / Delete" authority.
- Full Control
  This is a user granted full control.
- Registered User
  This is a user whose personal information is registered in the address book. The registered user is the user who knows the login user name and password.
- User Administrator
  This is the user administrator.

❍=You can view and change the setting.

▲=You can view the setting.

-=You cannot view or specify the setting.

Settings		User			User Administrator	Registered User	Full Control
		Read-only	Edit	Edit / Delete			
Regist No.		▲	❍	❍	❍	❍	❍
Name		▲	❍	❍	❍	❍	❍
Auth. Info	User Code	-	-	-	❍	-	-
	Login User Name	-	-	-	❍	▲	-
	Login Password	-	-	-	❍ *1	❍ *1	-
	Permit Function on Auth	-	-	-	❍	▲	-
Auth. Protect	Dest. Protection Object	-	-	-	❍	❍	❍

*1 You can only enter the password.

User Settings

If you have specified administrator authentication, the available functions and settings depend on the menu protect setting.

The following settings can be specified by someone who is not an administrator.

❍ =You can view and change the setting.

▲ =You can view the setting.

- =You cannot view or specify the setting.

Note

❒ Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

Panel Menu

The default for **[Menu Protect]** is **[Level 2]**.

Tab Names	Settings	Menu Protect		
		Off	Level 1	Level 2
Paper Input	All Settings	❍	❍	▲
Maintenance	Colour Registration	❍	▲	▲
	Colour Calibration	❍	▲	▲
	Registration	❍	▲	▲
	4 Colour Graphic Mode	❍	▲	▲
	Plain Paper	❍	❍	▲
	Letterhead	❍	❍	▲
	Glossy Paper	❍	❍	▲
	Coated Paper	❍	❍	▲
	Label Paper	❍	❍	▲
	Envelope	❍	❍	▲
	Replacement Alert	❍	▲	▲
	Supply End Option	❍	▲	▲
	Display Supply Info	❍	▲	▲
	Unit of Measure	❍	▲	▲
	Panel Key Sound	❍	▲	▲
	Warm-up Beeper	❍	▲	▲
	Display Contrast	❍	▲	▲
	Key Repeat	❍	▲	▲
	Auto Reset Timer	❍	▲	▲

Tab Names	Settings	Menu Protect		
		Off	Level 1	Level 2
Maintenance	Set Date	❍	▲	▲
	Set Time	❍	▲	▲
	Delete All Temporary Jobs	❍	▲	▲
	Delete All Stored Jobs	❍	▲	▲
	Auto Delete Temporary Jobs	❍	▲	▲
	Auto Delete Stored Jobs	❍	▲	▲
System	Print Error Report	❍	▲	▲
	Auto Continue	❍	▲	▲
	Memory Overflow	❍	▲	▲
	Printer Language	❍	▲	▲
	Error Display Setting	❍	▲	▲
	Sub Paper Size	❍	▲	▲
	Default Printer Lang.	❍	▲	▲
	Energy Saver	❍	▲	▲
	Memory Usage	❍	▲	▲
	B&W Page Detect	❍	▲	▲
	Spool Printing	❍	▲	▲
	RAM Disk	❍	▲	▲
	Notify by Email	❍	▲	▲
Print Settings	Copies	❍	▲	▲
	Page Size	❍	❍	▲
	Edge to Edge Print	❍	▲	▲
	Duplex	❍	▲	▲
	Rotate by 180 Degrees	❍	▲	▲
	Blank Page Print	❍	▲	▲
	Letterhead Setting	❍	▲	▲
	Bypass Tray Priority	❍	▲	▲
	Tray Switching	❍	▲	▲
	PCL Menu	❍	▲	▲
	PS Menu	❍	▲	▲
	PDF Menu	❍	▲	▲
Host Interface	All Settings	❍	▲	▲

Web Image Monitor Setting

❖ Device Settings

The settings available to the user depend on whether or not administrator authentication has been specified.
If administrator authentication has been specified, the settings available to the user depend on whether or not "Available Settings" has been specified.

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
System	Device Name	▲	❍	-
	Comment	▲	❍	-
	Location	▲	❍	-
	Spool Printing	▲	❍	-
	Protect Printer Display Panel	-	❍	-
	Display Panel Language	▲	❍	-
	Permit ROM Update	-	❍	-
	Display IP Address on Device Display Panel	-	❍	-
Paper	Paper Size	▲	❍	-
	Custom Paper Size	▲	❍	-
	Paper Type	▲	❍	-
	Paper Thickness	-	❍	-
	Apply Auto Paper Select	▲	❍	-
Date/Time	Set Date	▲	❍	-
	Set Time	▲	❍	-
	SNTP Server Address	▲	❍	-
	SNTP Polling Interval	▲	❍	-
	Time Zone	▲	❍	-

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
Timer	Energy Saver Mode	▲	❍	-
	Energy Saver Mode Timer	▲	❍	-
	Auto Reset Timer	▲	❍	-
	Auto Logout Timer	▲	❍	-
Logs	Collect Job Logs	-	❍	-
	Collect Access Logs	-	❍	-
	Transfer Logs	-	❍	-
	Encrypt Logs	-	❍	-
	Delete All Logs	-	❍	-
E-mail	Administrator E-mail Address	▲	❍	-
	Reception Protocol	▲	❍	-
	E-mail Reception Interval	▲	❍	-
	E-mail Storage in Server	▲	❍	-
	SMTP Server Name	▲	❍	-
	SMTP Port No.	▲	❍	-
	SMTP Authentication	▲	❍	-
	SMTP Auth. E-mail Address	▲	❍	-
	SMTP Auth. User Name	-	❍	-
	SMTP Auth. Password *1	-	❍	-
	SMTP Auth. Encryption	▲	❍	-
	POP before SMTP	▲	❍	-
	POP E-mail Address	▲	❍	-
	POP User Name	-	❍	-
	POP Password *1	-	❍	-
	Timeout setting after POP Auth.	▲	❍	-
	POP3/IMAP4 Server Name	▲	❍	-
	POP3/IMAP4 Encryption	▲	❍	-

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
E-mail	POP3 Reception Port No.	▲	❍	-
	IMAP4 Reception Port No.	▲	❍	-
	SMTP Reception Port No.	▲	❍	-
	E-mail Notification E-mail Address	▲	❍	-
	Receive E-mail Notification	-	❍	-
	E-mail Notification User Name	-	❍	-
	E-mail Notification Password	-	❍	-
Auto E-mail Notification	Notification Message	-	❍	-
	Group 1 and Group 4	-	❍	-
	Call Service	-	❍	-
	Out of Toner	-	❍	-
	Toner Almost Empty	-	❍	-
	Replacement Required: Maintenance Kit	-	❍	-
	Paper Misfeed	-	❍	-
	Cover Open	-	❍	-
	Out of Paper	-	❍	-
	Almost Out of Paper	-	❍	-
	Paper Tray Error	-	❍	-
	Output Tray Full	-	❍	-
	Unit Connection Error	-	❍	-
	Replacement Required: PCU	-	❍	-
	Used Toner Bottle is Full	-	❍	-
	Used Toner Bottle is Almost Full	-	❍	-
	Replacement Required: Transfer Unit	-	❍	-
	Replace PCU Soon	-	❍	-
	File Storage Memory Full Soon	-	❍	-
	Replace Transfer Unit Soon	-	❍	-

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
Auto E-mail Notification	Replace Maintenance Kit Soon	-	❍	-
	Log Error	-	❍	-
	Select Groups/Items to Notify	-	❍	-
On-demand E-mail Notification	Use On-demand E-mail Notification	-	❍	-
	Notification Subject	-	❍	-
	Notification Message	-	❍	-
	Access Restriction to Information	-	❍	-
	Receivable E-mail Address/Domain Name	-	❍	-
	E-mail Language	-	❍	-
User Authentication Management	User Authentication Management	-	❍	-
	User Code - Available Function	-	❍	-
	Basic Authentication - Printer Job Authentication	-	❍	-
	Windows Authentication - Printer Job Authentication	-	❍	-
	Windows Authentication - Domain Name	-	❍	-
	Windows Authentication - Group Settings for Windows Authentication	-	❍	-
	LDAP Authentication - Printer Job Authentication	-	❍	-
	LDAP Authentication - LDAP Authentication	-	❍	-
	LDAP Authentication - Login Name Attribute	-	❍	-
	LDAP Authentication - Unique Attribute	-	❍	-
	Integration Server Authentication - Printer Job Authentication	-	❍	-
	Integration Server Authentication - Integration Server Name	-	❍	-
	Integration Server Authentication - Authentication Type	-	❍	-
	Integration Server Authentication - Obtain URL	-	❍	-

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
User Authentication Management	Integration Server Authentication - Domain Name	-	❍	-
	Integration Server Authentication - Group Settings for Integration Server Authentication	-	❍	-
Administrator Authentication Management	User Administrator Authentication	-	❍	-
	Machine Administrator Authentication	-	❍	-
	Network Administrator Authentication	-	❍	-
	File Administrator Authentication	-	❍	-
Program/Change Administrator	User Administrator, Machine Administrator, Network Administrator, File Administrator	-	❍	-
	Login User Name - Administrator 1- 4	-	❍	-
	Login Password - Administrator 1- 4	-	❍	-
	Encryption Password - Administrator 1- 4	-	❍	-
	Login User Name - Supervisor	-	-	-
	Login Password - Supervisor	-	-	-
LDAP Server	Program/Change/Delete	-	❍	-

*1 You can only specify the password.

❖ Printer

The settings available to the user depend on whether or not administrator authentication has been specified.
If administrator authentication has been specified, the settings available to the user depend on whether or not "Available Settings" has been specified.

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
Basic Settings	Misfeed Recovery	-	❍	-
	Print Error Report	▲	❍	-
	Auto Continue	▲	❍	-
	Memory Overflow	▲	❍	-
	Auto Delete Temporary Print Jobs	▲	❍	-
	Auto Delete Stored Print Jobs	▲	❍	-
	Initial Print Job List	▲	❍	-
	Rotate by 180 Degrees	▲	❍	-
	Memory Usage	▲	❍	-
	Duplex	-	❍	-
	Copies	-	❍	-
	Blank Page Print	-	❍	-
	B&W Page Detect	-	❍	-
	Edge Smoothing	-	❍	-
	Toner Saving	-	❍	-
	Spool Image	-	❍	-
	Printer Language	-	❍	-
	Sub Paper Size	▲	❍	-
	Page Size	-	❍	-
	Letterhead Setting	▲	❍	-
	Bypass Tray Setting Priority	▲	❍	-
	Edge to Edge Print	-	❍	-
	Default Printer Language	-	❍	-
	List/Test Print Lock	-	❍	-

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
Basic Settings	I/O Buffer	▲	❍	-
	I/O Timeout	▲	❍	-
	Orientation - PCL	-	❍	-
	Form Lines - PCL	-	❍	-
	Font Source - PCL	-	❍	-
	Font Number - PCL	-	❍	-
	Point Size - PCL	-	❍	-
	Font Pitch - PCL	-	❍	-
	Symbol Set - PCL	-	❍	-
	Courier Font - PCL	-	❍	-
	Extend A4 Width - PCL	-	❍	-
	Append CR to LF - PCL	-	❍	-
	Resolution - PCL	-	❍	-
	Data Format - PS	-	❍	-
	Resolution - PS	-	❍	-
	Color Setting - PS	-	❍	-
	Color Profile - PS	-	❍	-
	Resolution - PDF	-	❍	-
	Color Setting - PDF	-	❍	-
	Color Profile - PDF	-	❍	-

❖ Interface

The settings available to the user depend on whether or not administrator authentication has been specified.
If administrator authentication has been specified, the settings available to the user depend on whether or not "Available Settings" has been specified.

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
Interface Settings	Change Interface	▲	-	-
	Network	▲	▲	-
	MAC Address	▲	▲	-
	Bluetooth	▲	❍	-
	Operation Mode	▲	❍	-
	USB	▲	❍	-
	USB Host	▲	❍	-
	PictBridge	▲	❍	-
Wireless LAN Settings	Change Interface	-	❍	-
	Network	▲	▲	-
	MAC Address	▲	▲	-
	Wireless Signal Status	▲	▲	-
	Communication Mode	▲	❍	-
	SSID	-	❍	-
	Channel	▲	❍	-
	Security Type	-	❍	-
	WEP Authentication	-	❍	-
	WEP Key Number	-	❍	-
	WEP Key	-	❍	-
	WPA Encryption Method	-	❍	-
	WPA Authentication Method	-	❍	-
	WPA-PSK	-	❍	-
	WPA (802.1X)	-	❍	-
	WPA Client Certificate	-	❍	-

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
Wireless LAN Settings	Password	-	❍	-
	Phase 2 User Name	-	❍	-
	Phase 2 Method (EAP-TTLS)	-	❍	-
	Phase 2 Method (PEAP)	-	❍	-
	Authenticate Server Certificate	-	❍	-
	Trust Intermediate Certificate Authority	-	❍	-
	Server ID	-	❍	-

*1 The IEEE802.11b interface unit option must be installed.

❖ Network

The settings available to the user depend on whether or not administrator authentication has been specified.
If administrator authentication has been specified, the settings available to the user depend on whether or not "Available Settings" has been specified.

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
IPv4	Host Name	❍	❍	▲
	DHCP	❍	❍	▲
	Domain Name	❍	❍	▲
	IPv4 Address	❍	❍	▲
	Subnet Mask	❍	❍	▲
	DDNS	❍	❍	▲
	WINS	❍	❍	▲
	Primary WINS Server	❍	❍	▲
	Secondary WINS Server	❍	❍	▲
	Scope ID	❍	❍	▲
	Default Gateway Address	❍	❍	▲
	DNS Server	❍	❍	▲
	LPR	❍	❍	▲
	RSH/RCP	❍	❍	▲
	DIPRINT	❍	❍	▲
	FTP	❍	❍	▲
	sftp	❍	❍	▲
	IPP	❍	❍	▲
	IPP Timeout	❍	❍	▲
IPv6	Host Name	❍	❍	▲
	Domain Name	❍	❍	▲
	Stateless Address Autoconfiguration	❍	❍	▲
	Manual Configuration Address	❍	❍	▲
	DDNS	❍	❍	▲

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
IPv6	Default Gateway Address	❍	❍	▲
	DNS Server 1-3	❍	❍	▲
	LPR	❍	❍	▲
	RSH/RCP	❍	❍	▲
	DIPRINT	❍	❍	▲
	FTP	❍	❍	▲
	sftp	❍	❍	▲
	IPP	❍	❍	▲
	IPP Timeout	❍	❍	▲
NetWare	NetWare	❍	❍	▲
	Print Server Name	❍	❍	▲
	Logon Mode	❍	❍	▲
	File Server Name	❍	❍	▲
	NDS Tree	❍	❍	▲
	NDS Context Name	❍	❍	▲
	Operation Mode	❍	❍	▲
	Remote Printer No.	❍	❍	▲
	Job Timeout	❍	❍	▲
	Frame Type	❍	❍	▲
	Print Server Protocol	❍	❍	▲
	NCP Delivery Protocol	❍	❍	▲
AppleTalk	AppleTalk	❍	❍	▲
	Printer Name	❍	❍	▲
	Zone Name	❍	❍	▲

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
SMB	SMB	❍	❍	▲
	Workgroup Name	❍	❍	▲
	Computer Name	❍	❍	▲
	Comment	❍	❍	▲
	Notify Print Completion	❍	❍	▲
SNMP	SNMP	❍	❍	▲
	IPv4	❍	❍	▲
	IPv6	❍	❍	▲
	IPX	❍	❍	▲
	SNMPv1/v2 Function	❍	❍	▲
	SNMPv1 Trap Communication	❍	❍	▲
	SNMPv2 Trap Communication	❍	❍	▲
	Permit Settings by SNMPv1 and v2	❍	❍	▲
	Community	❍	❍	▲
SNMPv3	SNMP	❍	❍	▲
	IPv4	❍	❍	▲
	IPv6	❍	❍	▲
	IPX	❍	❍	▲
	SNMPv3 Function	❍	❍	▲
	SNMPv3 Trap Communication	❍	❍	▲
	Authentication Algorithm	❍	❍	▲
	Permit SNMPv3 Communication	❍	❍	▲
	SNMPv3 Trap Communication Setting	❍	❍	▲
SSDP	SSDP	❍	❍	▲
	UUID	❍	❍	▲
	Profile Expires	❍	❍	▲
	TTL	❍	❍	▲

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
Bonjour	Bonjour	❍	❍	▲
	Computer Name	❍	❍	▲
	Location	❍	❍	▲
	DIPRINT	❍	❍	▲
	LPR	❍	❍	▲
	IPP	❍	❍	▲

❖ Security

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
Network Security	Security Level	-	❍	-
	TCP/IP	-	❍	-
	HTTP - Port 80	-	❍	-
	IPP - Port 80, Port 631	-	❍	-
	SSL/TLS - Port 443	-	❍	-
	SSL/TLS - Permit SSL/TLS Communication	-	❍	-
	SSL/TLS - Certificate Status	-	❍	-
	DIPRINT, LPR, FTP, sftp, ssh, RSH/RCP, TELNET, Bonjour, SSDP, BMLinkS, SMB, NetBIOS over TCP/IPv4	-	❍	-
	NetWare	-	❍	-
	AppleTalk	-	❍	-
	Permit Settings by SNMPv1 and v2	-	❍	-
	SNMPv1/v2 Function	-	❍	-
	SNMPv3 Function	-	❍	-
	Permit SNMPv3 Communication	-	❍	-
Access Control	Access Control Range 1 to Access Control Range 5 - IPv4	-	❍	-
	Access Control Range 1 to Access Control Range 5 - IPv6	-	❍	-
IPP Authentication	Authentication	-	❍	-
	User Name	-	❍	-
	Password	-	❍	-
SSL/TLS	SSL/TLS	-	❍	-
	Permit SSL/TLS Communication	-	❍	-
	Certificate Status	-	❍	-

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
ssh	ssh	-	❍	-
	Compression Transfer	-	❍	-
	Port Number	-	❍	-
	Timeout	-	❍	-
	Login Timeout	-	❍	-
	Public Key	-	❍	-
Site Certificate	Site Certificate Check	-	❍	-
	List of display items	-	❍	-
	Site Certificate to Import	-	❍	-
Device Certificate	List of display items	-	❍	-
	Explanation	-	❍	-
	Application	-	❍	-
	Usage Certificate	-	❍	-

Functions That Require Options

The following functions require certain options and additional functions.

- Basic Authentication, Windows Authentication, LDAP Authentication, Integration Server Authentication
  Printer Hard Disk Drive
- Server Certificate
  Hard disk or server certificate SD card.

INDEX

R

S

T

U

W

Operating Instructions Security Guide

GB (GB)
EN (USA) G160-8617A